SCDP 2-01.3 Intelligence Preparation of the Operational Environment

Security Corps Doctrine Publication

The Security Corps
September 2025

Table of Contents

Foreword....6
Preface....8
Scope and Applicability....8
Relationship to Other Doctrine....8
Guidance for Use....9
Introduction: The Proactive Advantage Through Understanding....10
Defining IPOE for the Security Corps....10
The Nature of the SC’s Operational Environment....11
IPOE in the SC Action Cycle....11
PART ONE: FUNDAMENTALS AND THE IPOE PROCESS....13
Chapter 1: The IPOE Framework....14
1-1. Introduction....14
1-2. The Four-Step Process....14
1-3. IPOE and Adaptive Command....15
1-4. The Central Role of PMESII-PT....16
1-5. The Living File Concept....17
1-6. Staff Collaboration (Adapted for the SC)....18
Chapter 2: Step 1 - Define the Operational Environment....19
2-1. Introduction....19
2-2. Purpose of Step 1....19
2-3. Identifying Geographic Boundaries: The Area of Operations and Area of Interest....19
2-4. Practical Application: Defining AO and AI for SC Missions....20
2-5. Analyzing the Mission and ENA/SC Leader’s Intent....21
2-6. Identifying Significant Characteristics of the Operational Environment....22
2-7. Identifying Intelligence Gaps and Initial Information Requirements....23
2-8. The Output of Step 1: The Foundation for Analysis....23
2-9. Conclusion....24
Chapter 3: Step 2 - Describe Environmental Effects on Operations....25
3-1. Introduction....25
3-2. The Physical Environment (Terrain & Weather)....25
3-3. Terrain Analysis (OAKOC/KOCOA)....25
3-4. Weather Analysis....28
3-5. Synthesizing the Physical Environment: The MCOO and Effects Matrices....28

3-6. The Information Environment....29
3-7. The Media Landscape....30
3-8. Formal and Informal Networks....30
3-9. The Online Environment....30
3-10. Synthesizing the Information Environment....31
3-11. Conclusion....31
Chapter 4: Step 2 (Continued) - Describe Environmental Effects on Operations (The Human Domain)....32
4-1. Introduction....32
4-2. The Social Environment: The Fabric of the Community....32
4-3. The Political Environment: The Structures of Power....35
4-4. The Economic Environment: The Flow of Resources....36
4-5. The Output: A Multi-Layered Understanding of the Human Terrain....37
4-6. Conclusion....37
PART TWO: THREAT ANALYSIS AND OPERATIONAL APPLICATION....38
Chapter 5: Step 3 - Evaluate the Threat....39
5-1. Introduction....39
5-2. Defining “Threat” in the SC Context....39
5-3. Identifying Threat Characteristics....39
5-4. Creating Threat Models....41
5-5. The Output of Step 3: A Portfolio of Threat Models....43
5-6. Conclusion....43
Chapter 6: Step 4 - Determine Threat Courses of Action (COAs)....45
6-1. Introduction....45
6-2. Identifying Threat Objectives and Desired End State....45
6-3. Developing the Full Set of Threat COAs....46
6-4. Evaluating and Prioritizing Threat COAs....46
6-5. Developing the COA in Detail....47
6-6. Developing the Event Template and Event Matrix....48
6-7. The Output of Step 4: Predictive Intelligence....49
6-8. Conclusion....49
Chapter 7: IPOE and the SC Planning Process....51
7-1. Introduction: From Understanding to Action....51
7-2. Supporting Mission Analysis (TLP Step 1 & 3)....51
7-3. Supporting Friendly Course of Action (COA) Development (TLP Step 3)....52

7-4. Supporting Wargaming (TLP Step 4)....53
7-5. Developing the Information Gathering Plan....53
7-6. Supporting Assessment....54
7-7. Conclusion....55
Chapter 8: The Living File - Continuous Assessment....56
8-1. Introduction....56
8-2. The Study is Never “Finished”: From Static Product to Living File....56
8-3. The Assessment Cycle: A Habit of Mind....57
8-4. Indicators and Warnings (I&W): Your Tripwire System....58
8-5. A Sustainable Routine for Volunteers....59
8-6. Conclusion....60
Conclusion: The Proactive Advantage....61
Appendix A: Glossary of Key Terms....64
Appendix B: IPOE Process Checklists....68
B-1. Purpose....68
Checklist 1: Step 1 - Define the Operational Environment....68
Checklist 2: Step 2 - Describe Environmental Effects....70
Checklist 3: Step 3 - Evaluate the Threat....71
Checklist 4: Step 4 - Determine Threat Courses of Action (COAs)....72
Appendix C: Sample IPOE Products....75
C-1. Purpose....75
Template 1: SC Modified Combined Obstacle Overlay (MCOO)....75
Template 2: SC Threat Model Fact Sheet....76
Template 3: SC Situation Template (SITEMP)....77
Template 4: SC Event Template and Event Matrix....78
Appendix D: Comprehensive PMESII-PT Collection Checklist....80
D-1. Purpose....80
D-2. How to Use This Checklist....80
(P) - Political....80
(M) - Military (Law Enforcement & Emergency Services)....81
(E) - Economic....82
(S) - Social....82
(I) - Information....83
(I) - Infrastructure....83
(P) - Physical Environment....84

(T) - Time....84
Appendix E: Legal Compliance in IPOE Reminder....86
E-1. The Non-Negotiable Foundation....86
E-2. Core Principles of Lawful Intelligence Gathering....86
E-3. Strictly Prohibited Activities....86
E-4. Specific Considerations for Key Collection Activities....87
E-5. The Leader’s Responsibility....87
E-6. Final Admonition....87

Foreword

The ability of the Euramerican Security Corps to generate Protective Power—our unique capacity to lawfully create and sustain a secure environment for our community—is not derived from brute force, but from superior awareness and preparation. Foresight is our greatest weapon, and knowledge is our most vital shield. It is this fundamental principle that lies at the heart of our intelligence doctrine and is the subject of this essential publication, SCDP 2-01.3, *Intelligence Preparation of the Operational Environment*. The methodology contained within these pages is the intellectual engine that drives our vigilance, informs our planning, and enables the proactive safeguarding of our people.

This publication is not a reinvention of intelligence doctrine, but a deliberate and meticulous adaptation of a proven, professional-grade methodology to the unique mission of the Security Corps. We are not a state military operating with sovereign authority, but a lawful, auxiliary security element serving the Euramerican national community. We function within complex legal landscapes, rely on the commitment of dedicated volunteers, and depend utterly on the trust of the community we protect. This context demands a tailored approach to understanding our environment—one that is rigorous in its analysis, realistic in its application, and relentlessly focused on our core protective mandate. SCDP 2-01.3 provides that specific approach.

The methodology detailed herein is not an end in itself; it is a tool forged for a single, solemn purpose: to enable us to better safeguard the Euramerican national community, its rights, and its future. The process of Intelligence Preparation of the Operational Environment (IPOE) transforms us from passive observers into active analysts. It is the intellectual work that precedes and enables responsible physical action, ensuring that our efforts are focused, our resources are stewarded wisely, and our plans are grounded in a deep and functional knowledge of the terrain, the information landscape, and the human dynamics of our Area of Operations.

Let me be unequivocal on a point of paramount importance, which is woven into every chapter of this manual and must be embedded in every action you take. Our legitimacy, our operational freedom, and the very trust of the community we serve depend on our unwavering commitment to the rule of law. Therefore, the absolute and non-negotiable imperative of lawful operation must govern every facet of our intelligence activities. The collection of information, the conduct of surveillance, and the analysis of data will, at all times and without exception, be conducted in strict compliance with the laws of the jurisdiction in which we operate. There is no operational objective that can ever justify unlawful methods. Adherence to this principle is the bedrock of our honor and the guarantor of our continued existence.

I therefore direct every member of the Security Corps, particularly our Commissioned leaders and those entrusted with planning and intelligence functions, to study this doctrine diligently. Internalize its processes and apply its principles with discipline and sound judgment. By doing so, you will become a more capable analyst, a more effective planner, and a more responsible guardian of our community. Through the mastery of these principles, we will sharpen our vigilance, enhance our readiness, and solidify our ability to provide effective, lawful protection for generations to come.

[Name and Title] Commander, ENA Security Corps [Date]

Preface

This publication, Security Corps Doctrine Publication (SCDP) 2-01.3, establishes the authoritative doctrine for the conduct of Intelligence Preparation of the Operational Environment (IPOE) within the Euramerican Security Corps. Planning and executing effective, lawful security operations requires a profound and continuous understanding of the environment in which we function. The IPOE process is the systematic methodology through which we achieve that understanding. Its purpose is to provide our leaders and members with a shared framework for analyzing threats, terrain, weather, and the complex human domain, enabling the proactive security and informed decision-making necessary to fulfill our protective mission for the Euramerican National Assembly (ENA).

Scope and Applicability

The principles and procedures detailed herein apply to all members and echelons of the Euramerican Security Corps, across the full spectrum of our potential activities. While the primary audience is our Commissioned leaders and those personnel assigned to intelligence, planning, and security roles, a fundamental grasp of this doctrine is essential for all members who contribute to or execute our plans.

This publication is the detailed "how-to" manual for the SC's intelligence process. It directly expands upon the foundational concepts of Protective Intelligence introduced in SCDP 2-0, *Security Corps Intelligence*. Where SCDP 2-0 explains the "what and why" of our intelligence function, this document provides the specific, step-by-step methodology for "how" we prepare the battlefield. It is designed to be a practical guide, translating the theory of intelligence into the tangible products that drive operational success.

Relationship to Other Doctrine

SCDP 2-01.3 is an integral part of the Security Corps' doctrinal library and must be understood in its relationship to other core publications. It is fundamentally nested under the overarching principles of our organization and mission as defined in SCDP 1, *The Security Corps,* and the core intelligence concepts of SCDP 2-0, *Security Corps Intelligence*.

This doctrine directly supports and enables the processes detailed in our operational manuals:

- It provides the situational understanding upon which all sound operational planning, as detailed in SCDP 5-0, *Planning*, is based. The IPOE process is the engine that drives the adapted Troop Leading Procedures (TLP).
- It informs the development and execution of all activities described in SCDP 3-0, *Operations*, ensuring our actions are grounded in a realistic appreciation of the environment and potential threats.
- It provides the essential context and situational awareness necessary for leaders to exercise the principles of Adaptive Command detailed in SCDP 6-0, *Command and Control*.

The terminology used herein is consistent with that defined in the SC Glossary to ensure a common language across our force. The IPOE process itself constitutes the core of the "Observe"

and “Orient” phases of the OODA loop and is the primary activity that informs the “Plan” phase of the SC Action Cycle (Plan-Prepare-Act-Assess).

Guidance for Use

This doctrine provides the authoritative framework for thought and action regarding Intelligence Preparation of the Operational Environment. It is not, however, a rigid checklist to be followed without critical thought, nor is it a substitute for sound judgment. The art of intelligence lies in the skillful application of this scientific process to the unique circumstances of each situation. Leaders and members must exercise intellectual rigor, creativity, and adaptability when applying these principles, tailoring the depth and focus of their IPOE effort to the time available, the complexity of the mission, and the specific directives of the ENA.

Above all, this doctrine must be viewed through the non-negotiable lens of absolute legal compliance. The Security Corps operates lawfully, or it does not operate at all. Every principle, technique, and procedure described in this manual must be applied in a manner that fully and unequivocally adheres to the laws of the jurisdiction in which we are present. A plan derived from an IPOE that contemplates or risks unlawful action is fundamentally flawed and invalid. The responsibility for ensuring this adherence rests with every leader and member involved in the process.

The proponent for SCDP 2-01.3 is the Security Corps Headquarters Intelligence Staff. We encourage recommendations for improving this publication, as our doctrine must remain a living body of knowledge, refined by experience and thoughtful feedback. Please submit recommendations through the established SC chain of command.

Introduction: The Proactive Advantage Through Understanding

In any contest, the victor is almost always the one who can make better decisions, faster. This timeless principle, that knowledge is power, is the bedrock of all effective security operations. For the Euramerican Security Corps, this is not an abstract slogan; it is a fundamental tenet that guides our every action. As established in foundational texts like *The Area Study*, our ability to safeguard the Euramerican community is directly proportional to our ability to out-think and out-maneuver potential threats. This intellectual superiority is achieved through the disciplined application of the OODA Loop: **Observe, Orient, Decide, and Act**.

Every rational actor, from a security team responding to an alarm to a family preparing for a storm, cycles through this process. We **Observe** the unfolding situation, gathering raw data from our environment. We then **Orient** ourselves to that data, a critical and often-overlooked step where we analyze and synthesize the information, compare it against our existing knowledge, and build a coherent mental model of reality. It is in the orientation phase that we make sense of chaos, identify threats, and recognize opportunities. Based on this orientation, we **Decide** on a lawful course of action. Finally, we **Act**, putting our decision into motion. The results of that action then create a new set of observations, and the cycle begins again.

The genius of this model lies in the understanding that victory belongs to whoever can cycle through the OODA Loop more effectively than their opponent. However, the quality of the entire loop hinges on the strength of its first two stages. A decision based on flawed observation or a poor orientation is destined to fail, no matter how swiftly it is executed. To act decisively and lawfully, we must first see the world clearly and understand it deeply. Intelligence Preparation of the Operational Environment (IPOE) is the Security Corps' systematic, professional-grade methodology for mastering these critical Observe and Orient phases. It is the process that forges the proactive advantage.

Defining IPOE for the Security Corps

The Security Corps adapts the proven IPOE process to our specific protective mission. We therefore define Intelligence Preparation of the Operational Environment as:

The systematic, continuous process of analyzing the threat and the environmental variables of Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-PT) within a specific Area of Operations to determine their effect on the Security Corps' ability to safeguard the Euramerican national community, its rights, and its future.

This process is fundamentally analytical. It is not merely the collection of facts to fill a binder. A list of roads, a census report, and a list of local political groups are data points. In their isolated state, they are of limited value. IPOE is the rigorous intellectual work that transforms this raw data into actionable intelligence by relentlessly asking the question, "So what?" It is the process of understanding that a specific political group (**Political**) is planning a protest at the courthouse, which is located at a major transportation chokepoint (**Infrastructure**), on the same day as a large cultural festival (**Social/Time**), creating a high potential for conflict that will overwhelm the capabilities of local law enforcement (**Military**). This synthesized understanding—this intelligence—allows us to anticipate events rather than merely react to them, enabling us to

develop proactive, lawful security plans. The IPOE process, using the comprehensive PMESII-PT framework, is how we build this deep, functional model of our environment.

The Nature of the SC's Operational Environment

The Security Corps does not operate in a conventional military context, which is precisely why we require our own tailored IPOE doctrine. Our operational environment is defined by a unique set of challenges that shape every aspect of our intelligence efforts. A disciplined IPOE process is the primary tool we use to navigate these complexities successfully.

- **Legal Complexity:** This is our most significant and non-negotiable constraint. The SC operates as a lawful, auxiliary security element across a patchwork of numerous federal, state, and local jurisdictions. Laws governing surveillance, privacy, freedom of assembly, and the possession and use of equipment can vary dramatically from one county to the next. Our IPOE process must therefore have an integrated and continuous legal analysis component to ensure every proposed action is meticulously vetted for compliance.
- **Community Embeddedness:** Unlike a military force deployed to a foreign land, we operate within and among the very community we are sworn to protect. This presents both unique opportunities and profound responsibilities. It allows for unparalleled access to local knowledge and the potential for trust-based, lawful Human Intelligence (HUMINT). However, it also demands the highest ethical standards in information handling, absolute discretion to protect privacy, and constant awareness of how our actions are perceived. Our IPOE must be sophisticated enough to analyze these social dynamics and maintain the community trust that is our center of gravity.
- **Volunteer Realities:** The SC is a force of dedicated volunteers. This reality imposes practical constraints on time, resources, and available equipment. Our IPOE process must be efficient, scalable, and focused. It must prioritize requirements ruthlessly, leveraging simple but effective tools to produce the necessary understanding without creating an unsustainable administrative burden. We must achieve professional-grade results within the practical limits of a volunteer organization.
- **The Modern Information Environment:** We operate in an age of information saturation, where misinformation (unintentional falsehoods) and disinformation (deliberate propaganda) can spread instantly. Our IPOE process must be rigorous enough to vet sources, corroborate information, identify hostile narratives, and provide our leaders with the clearest possible picture of the truth amidst the noise, as detailed in SCDP 2-0, *Security Corps Intelligence*.

IPOE in the SC Action Cycle

Intelligence Preparation of the Operational Environment is not a one-time, pre-mission activity. It is a continuous and cyclical process that is fully integrated with every phase of the SC Action Cycle: **Plan-Prepare-Act-Assess**. IPOE is the cognitive engine that powers this cycle.

- **Supporting the Plan Phase:** IPOE is the foundation of all sound planning. The detailed analysis of the operational environment (METT-TC) derived from the IPOE process provides the essential understanding needed to formulate feasible, acceptable, suitable, and, above all, lawful friendly Courses of Action (COAs), as detailed in SCDP 5-0, *Planning*.

- **Informing the Prepare Phase:** As we prepare for an operation, the IPOE product provides the necessary context. It informs our rehearsals by highlighting the most likely or most dangerous threat COAs. It focuses our pre-mission checks by identifying specific environmental challenges (e.g., weather, terrain) or legal constraints that require special attention.
- **Guiding the Act (Execution) Phase:** During execution, the situation is in constant flux. The IPOE process provides ongoing situational awareness, allowing leaders to assess changes, identify emerging threats or opportunities, and make timely and informed decisions. It provides the understanding necessary to exercise Disciplined Initiative within the framework of Adaptive Command, as described in SCDP 6-0, *Command and Control*.
- **Enabling the Assess Phase:** Assessment measures the progress of an operation against its objectives. The IPOE provides the critical baseline picture of the operational environment. By comparing the current situation to the baseline established during IPOE, we can effectively measure the impact of our actions, evaluate our effectiveness, and identify lessons learned that will feed back into the next planning cycle.

In conclusion, the IPOE process is the SC's fundamental methodology for developing the proactive advantage. It is how we transform our commitment to vigilance into a tangible, intellectual capability. It provides the deep, lawful, and functional understanding of our environment necessary to plan effectively, prepare intelligently, act decisively, and assess honestly. By mastering the doctrine contained within these pages, we equip ourselves with the knowledge required to fulfill our solemn mission: to lawfully safeguard the Euramerican national community, its rights, and its future.

PART ONE: FUNDAMENTALS AND THE IPOE PROCESS

Chapter 1: The IPOE Framework

1-1. Introduction

The successful execution of any Security Corps mission is predicated on a deep and functional understanding of the environment in which we operate. This understanding is not gained by chance or intuition alone; it is the product of a deliberate, structured, and continuous analytical effort. This chapter establishes the intellectual framework for that effort: the Security Corps' methodology for Intelligence Preparation of the Operational Environment (IPOE). This framework provides the essential blueprint for how we analyze complex situations, identify threats, and develop the situational awareness necessary to plan and act effectively and lawfully. It is comprised of a logical four-step process, is guided by the comprehensive PMESII-PT model, and is fully integrated with our command philosophy of Adaptive Command. Mastering this framework is the first and most critical step for any SC leader or member seeking to transform raw information into the proactive advantage that defines our Protective Power.

1-2. The Four-Step Process

The IPOE process provides a systematic and repeatable methodology for analyzing any operational environment. It is a logical sequence that guides the analyst from a broad, general understanding of the area to a specific, detailed assessment of potential threat actions. While presented as four distinct steps, the process is iterative and dynamic; insights gained in a later step often require the analyst to revisit and refine the products of an earlier one. This continuous loop of analysis ensures that our understanding remains relevant as new information becomes available.

Step 1: Define the Operational Environment

The purpose of this foundational step is to focus the overall intelligence effort by clearly defining the physical, temporal, and analytical boundaries of the mission. An unfocused effort wastes valuable time and resources on irrelevant information. This step ensures that our analysis is tailored precisely to the needs of the commander and the specific task at hand. Key activities include identifying the SC's Area of Operations (AO) and Area of Interest (AI), analyzing the mission assigned by higher ENA or SC echelons, and conducting an initial survey of the environment to identify its most significant characteristics. The primary output of this step is a clear understanding of the geographic area of concern and a prioritized list of initial Information Needs, which will guide the subsequent, more detailed, collection and analysis efforts. Success in this step prevents the analyst from being overwhelmed by the sheer volume of available data and channels their work toward what is truly important for mission success.

Step 2: Describe the Environmental Effects on Operations

Once the operational environment is defined, the purpose of Step 2 is to analyze how the significant characteristics of that environment affect the capabilities and broad courses of action for both our own SC elements and any potential threats. This step is about seeing the environment not as a static backdrop, but as an active participant that helps, hinders, and shapes the actions of everyone within it. The analysis is conducted through the comprehensive lens of

the PMESII-PT framework, examining how the Physical Environment (terrain, weather), the Information Environment (media, networks), and the Human Domain (social, political, economic factors) impact operations. For example, a dense urban area (**Infrastructure**) may degrade radio signals (**Information**) and canalize movement (**Physical**), while a politically charged local election (**Political/Time**) may create social tensions (**Social**) that could be exploited by hostile actors. The primary outputs of this step are analytical products like a Modified Combined Obstacle Overlay (MCOO), terrain and weather effects matrices, and assessments of the civil and information environments. This detailed analysis provides the essential context needed to realistically evaluate threat capabilities and develop sound, lawful friendly plans.

Step 3: Evaluate the Threat

The purpose of this step is to develop a deep understanding of each potential threat actor identified in Step 1, independent of the specific effects of the immediate operational environment. The goal is to build a comprehensive model of how a threat is organized, equipped, trained, and how it prefers to operate. For the SC, a "threat" could range from a hostile activist network or criminal element to potentially disruptive state actors. This evaluation involves a detailed analysis of the threat's characteristics, such as their composition, disposition, strength, leadership, logistics, and observed tactics, techniques, and procedures (TTPs). The key output of this step is a set of Threat Models for each significant potential adversary. A Threat Model typically consists of a graphic template depicting how the threat doctrinally organizes for a specific type of action, a narrative describing their preferred tactics and options, and a list of their High-Value Targets (HVTs)—those assets critical for their own success. A robust Threat Model allows us to understand our adversaries as they see themselves, preventing us from "mirror-imaging" our own tactics and assumptions onto them.

Step 4: Determine Threat Courses of Action (COAs)

This final step is the synthesis of all previous work. Its purpose is to integrate the detailed understanding of the threat (from Step 3) with the analysis of the operational environment's effects (from Step 2) to develop a set of specific, likely, and dangerous threat Courses of Action (COAs). This is where we predict what the adversary will actually *do* in this particular situation. The process involves identifying the threat's likely objectives, developing a full set of valid COAs they could take, and then evaluating and prioritizing them to determine which is the **Most Likely** and which is the **Most Dangerous** to the SC/ENA mission. Each of these priority COAs is then developed in detail, resulting in a **Situation Template (SITEMP)**—a graphic depicting the threat executing that specific COA on the actual terrain—and a supporting narrative. By comparing the different SITEMPs, we can identify unique indicators of each COA, leading to the creation of an **Event Template** and **Event Matrix**, which are the primary tools for focusing our ongoing intelligence collection efforts. This final step provides the predictive intelligence necessary for our leaders to develop and wargame effective, lawful friendly plans.

1-3. IPOE and Adaptive Command

The Security Corps' command and control philosophy is **Adaptive Command**, a framework that empowers subordinate leaders to exercise **Disciplined Initiative** within the commander's intent and strict legal boundaries (SCDP 6-0). This approach is essential for operating effectively in the complex and dynamic environments we face. Intelligence Preparation of the Operational

Environment is not merely a supporting process for Adaptive Command; it is the fundamental enabler that makes it possible.

Effective IPOE creates the essential conditions upon which Adaptive Command relies:

- **Shared Understanding:** The single greatest contribution of a thorough IPOE process is the creation of a deep and shared understanding of the operational environment across the SC element. When every member, from the leader to the newest Volunteer, has been briefed on the terrain, the civil considerations, the threat models, and the likely enemy COAs, they all operate from a common mental map. This shared context is the bedrock that allows decentralized elements to act in a coordinated and mutually supportive way, even with minimal communication, because they can anticipate the actions and needs of their comrades.
- **Meaningful Leader's Intent:** The Commander's Intent—the clear articulation of the mission's purpose, key tasks, and desired end state—is the cornerstone of Adaptive Command. A leader cannot formulate a meaningful and realistic intent in a vacuum. The IPOE process provides the leader with the necessary understanding of the situation to craft an intent that is grounded in reality. It allows the leader to identify the truly *key* tasks and to visualize an end state that is both achievable and lawful within the specific context.
- **Disciplined Initiative:** Initiative without knowledge is simply recklessness. The IPOE process provides the knowledge that disciplines initiative. When a subordinate leader encounters an unforeseen situation, their ability to take appropriate, lawful action is directly proportional to their understanding of the environment. A leader who understands the key terrain, the likely location of civilians, the threat's TTPs, and, most importantly, the established legal boundaries, is equipped to make sound decisions that support the intent. IPOE provides the "left and right limits" for action, ensuring that initiative remains productive and, above all, lawful.
- **Prudent Risk Management:** Adaptive Command requires leaders at all levels to assess and accept prudent risk. The IPOE process is the primary tool for this. It systematically identifies hazards and threats within the environment—operational, safety, and especially legal. By understanding the potential risks through IPOE, leaders can develop mitigation measures and make informed decisions about which risks are acceptable to achieve the mission and which are not. For the SC, a thorough IPOE is the first line of defense against incurring unacceptable legal risk.

In essence, IPOE provides the intellectual fuel for Adaptive Command. It replaces uncertainty with assessed knowledge, empowering our leaders and members to act with the confidence, agility, and responsibility required to succeed in our unique mission.

1-4. The Central Role of PMESII-PT

To ensure our analysis of the operational environment is comprehensive and holistic, the Security Corps utilizes the **PMESII-PT** framework as its primary analytical tool. First introduced in our foundational preparedness guide, *The Area Study*, this framework deconstructs any environment into its eight interrelated domains, serving as an intellectual checklist to prevent analytical blind spots and ensure no critical factor is overlooked.

- **Political:** Examines the distribution of power and governance. For the SC, this focuses

on local government structures, key elected officials, influential non-governmental groups, and, critically, the **Legal Framework** that defines our operational boundaries.

- **Military:** Analyzes the entities with an organized capacity for force. In our context, this primarily refers to local **Law Enforcement** agencies (their capabilities, jurisdictions, and response patterns) but also includes any military presence and, crucially, any ideologically motivated **threat groups** with paramilitary training or capabilities.
- **Economic:** Analyzes the production, distribution, and consumption of goods and services. Our focus is on identifying the area's key economic drivers, critical **supply chains**, and potential economic vulnerabilities that could lead to instability.
- **Social:** Examines the human terrain. This includes objective **demographics**, the local culture and religious landscape, and the sources of social cohesion and division. A critical component for the SC is the objective and dispassionate mapping of **extremist and activist groups** across the ideological spectrum to understand their potential to cause disruption.
- **Information:** Analyzes how knowledge and narratives are created, shared, and perceived. This involves mapping the formal **media landscape**, understanding informal "grapevine" networks, and assessing the online environment for **propaganda and disinformation** campaigns.
- **Infrastructure:** Covers the fundamental man-made systems that sustain the community. This analysis focuses on identifying critical nodes and chokepoints in transportation networks, the energy grid, water and sanitation systems, and communications infrastructure.
- **Physical Environment:** Analyzes the natural world, including topography, hydrography, climate, and weather. This is the domain where we apply the **OAKOC/KOCOA** framework to understand how the terrain impacts movement, observation, and security.
- **Time:** A unique, cross-cutting variable that examines how temporal factors influence all other domains. This includes daily rhythms (rush hour), seasonal changes (harvest, blizzards), the tempo of unfolding events, and the influence of **historical context** on current attitudes.

The true power of the PMESII-PT framework lies not in simply cataloging data within these eight domains, but in the synthesis—the analysis of how these domains interact. A change in the **Economic** domain (e.g., a factory closure) can lead to unrest in the **Social** domain, which is then amplified by the **Information** domain, creating a challenge for the **Political** and **Military (Law Enforcement)** domains, all of which is shaped by the physical layout of the **Infrastructure** and **Physical Environment**. This holistic, multi-domain perspective is the very essence of a superior orientation.

1-5. The Living File Concept

A critical mistake in any intelligence endeavor is to view the final product as a static, finished document. An IPOE, once completed, is not a historical record to be placed on a shelf; it is the baseline for a living intelligence file. The operational environment is in a constant state of flux. Political leaders change, economic conditions shift, new social tensions arise, and infrastructure is built or decays.

An IPOE that is not continuously updated quickly develops a "relevancy gap"—a dangerous delta between your understanding of the world and the world as it actually exists. Decisions

based on outdated intelligence are, by definition, flawed and carry immense risk.

Therefore, the IPOE process does not end with Step 4. It transitions into a continuous process of **Area Assessment**. This is the discipline of keeping the intelligence file current by systematically monitoring the environment, identifying significant changes, and updating the relevant sections of the IPOE product. This is the practical application of the “Assess” phase of the SC Action Cycle. Every new piece of credible information, whether from a news report, a patrol debrief, or a community interaction, must be evaluated for its impact on the existing IPOE. This requires establishing a sustainable routine for monitoring and updating, and using tools like Indicators and Warnings (I&W) to focus our attention. The IPOE is never “finished”; it is a dynamic tool that must evolve in parallel with the environment it describes.

1-6. Staff Collaboration (Adapted for the SC)

While large military organizations rely on formal, specialized staff sections to conduct IPOE, the Security Corps, as a smaller, volunteer-based force, achieves this through a collaborative mindset and the integration of functional expertise. The production of a comprehensive IPOE is not the responsibility of a single individual, but a team effort.

- **The Leader:** The SC leader (e.g., Team or Squad Leader) drives the IPOE process. They are the primary consumer of the intelligence and are ultimately responsible for its quality. The leader provides the initial focus, asks the critical questions (Information Needs), applies their own experience and judgment to the analysis, and makes the final decisions based on the product.
- **The Intelligence Role:** Within an SC element, one or more individuals (a designated Commissioned Member or an experienced Volunteer) may take the lead intelligence role. This individual is responsible for the detailed work of collection, analysis, and production —managing the data file, creating the overlays, and drafting the assessments under the leader’s guidance.
- **Every SC Member as a Sensor:** Our greatest intelligence asset is our network of dedicated members embedded within the community. Every member is a potential sensor, capable of providing valuable observations and local knowledge. The IPOE process must have a clear mechanism for members to report their observations lawfully and for that information to be integrated into the central intelligence picture.
- **Functional Expertise Integration:** A holistic IPOE requires input from members with diverse skills. The communications expert can analyze the local electromagnetic environment and identify signal dead zones (**Infrastructure/Information**). The sustainment expert can analyze logistical routes and supply chain vulnerabilities (**Economic/Infrastructure**). The medical expert can assess local health services and environmental health risks (**Social/Infrastructure**). The leader is responsible for drawing on this expertise during the planning process to enrich the IPOE.

This collaborative approach ensures that our IPOE products are not the product of a single, narrow perspective, but are a well-rounded synthesis of the collective knowledge and expertise of the entire SC element. It is through this disciplined, collaborative, and continuous framework that the Security Corps builds the superior understanding necessary to lawfully and effectively fulfill its protective mission.

Chapter 2: Step 1 - Define the Operational Environment

2-1. Introduction

The process of Intelligence Preparation of the Operational Environment begins with an act of discipline: the imposition of focus. An analyst faced with the infinite complexity of the modern world can easily become paralyzed, lost in a sea of data that is interesting but not relevant. The purpose of Step 1 is to prevent this failure by establishing clear and logical boundaries for our intelligence effort. It is the crucial first step that channels our limited time, resources, and analytical energy toward understanding only those factors that can meaningfully impact our ability to lawfully safeguard the Euramerican community.

Just as a surgeon must first define the precise surgical field before making an incision, the SC intelligence analyst must first define the operational environment. This involves delineating the geographic area of concern, deconstructing the assigned mission to understand its core requirements, and conducting an initial survey of the environment to identify its most significant characteristics. A failure to perform this step with diligence and precision will lead to a cascading series of errors: unfocused collection, irrelevant analysis, and ultimately, a flawed intelligence product that fails to support the leader's decision-making process. This chapter provides the methodology for building the solid foundation upon which all subsequent, detailed analysis will rest.

2-2. Purpose of Step 1

The overarching purpose of defining the operational environment is to focus the intelligence effort. This is achieved by accomplishing three primary objectives:

1. **To Define Geographic and Analytical Boundaries:** We cannot know everything about everywhere. This step forces us to define our geographic limits—the Area of Operations (AO) and Area of Interest (AI)—and to identify the most significant characteristics within those boundaries. This creates a manageable scope for our analysis.
2. **To Align with the Mission:** The IPOE process does not exist in a vacuum; it exists to support a specific mission. This step ensures our intelligence effort is directly tied to the tasks, purpose, and intent provided by ENA or higher SC command, guaranteeing that our final product will be relevant to the leader's needs.
3. **To Guide the Collection Effort:** By identifying what is already known versus what needs to be learned, this step allows us to formulate a set of initial Information Needs. These focused questions become the basis for a targeted and efficient information gathering plan, preventing us from wasting effort on collecting data that does not contribute to situational understanding.

2-3. Identifying Geographic Boundaries: The Area of Operations and Area of Interest

One of the first and most critical tasks in Step 1 is to define our geographic focus. We cannot study an entire state with the level of detail required for effective security operations. To prioritize our efforts, we adapt the professional concepts of the Area of Operations and the Area

of Interest, visualized through the “Bullseye” concept first introduced in *The Area Study*.

- **Area of Operations (AO):** The Area of Operations is the specific, defined geographic area where the SC element is assigned to conduct its mission. This is our primary focus, the ground we must know in intimate, granular detail. We must understand its backroads, its infrastructure, its people, and its legal landscape as if it were our own backyard. The majority of our collection and analysis efforts will be expended within the AO.
- **Area of Interest (AI):** The Area of Interest is the broader geographic region that contains threats, influences, or other factors that can affect operations within our AO. We do not need the same level of granular detail for our AI, but we must maintain strategic awareness of it. An event that occurs within our AI—such as a political decision at the state capital, a protest in a nearby major city, or the staging of a hostile group in an adjacent county—can have a direct and immediate impact on our AO. The AI provides the essential context for our primary analysis.

The **“Bullseye” Concept** is the simplest way to visualize and delineate these areas:

- **The Bullseye:** At the absolute center is the specific person, place, or asset being protected or the primary objective of the mission. This could be an ENA leader’s residence, a community meeting hall, or a critical piece of infrastructure.
- **The First Ring (The AO):** Surrounding the bullseye is the Area of Operations. Its boundaries are defined by the scope of the mission and the area the SC element can realistically influence and secure. For a static security mission, the AO might be the facility and its immediate perimeter. For a community monitoring mission, the AO might be an entire county.
- **The Outer Rings (The AI):** These rings represent the Area of Interest. As we move further from the center, the required level of detail decreases. We do not need to know every street name in a city 50 miles away, but we do need to know that the city exists, that it hosts a particular activist group, and that its major highway connects directly to our AO.

This tiered approach is a powerful tool for a volunteer force with limited time. It allows us to focus our most intensive efforts where they matter most—within our AO—while still maintaining the necessary situational awareness of the broader factors in our AI that could change our world in an instant.

2-4. Practical Application: Defining AO and AI for SC Missions

The specific boundaries of the AO and AI will change with every mission. Leaders must thoughtfully define these areas based on their analysis of the task at hand. The following examples illustrate this process for typical SC activities.

- **Mission: Event Security for an ENA Town Hall**
  - **Bullseye:** The community hall where the event is taking place.
  - **Area of Operations (AO):** The community hall itself, its entire property including parking lots, all points of entry and exit, and the immediately adjacent streets and public spaces from which direct observation or disruption of the event is possible. This is the area where the SC security element has direct responsibility for access

control, observation, and response.
    - **Area of Interest (AI):** The entire city or town where the event is located, the surrounding counties, and any known locations of potentially hostile groups within a reasonable travel distance (e.g., 1-2 hours). The AI must include the primary and alternate routes for ENA leadership and attendees traveling to the event, major transportation hubs (like train stations or airports if relevant), and the locations of local police, fire, and medical services.
- **Mission: Community Stability Monitoring for a County**
    - **Bullseye:** There may not be a single bullseye, but rather a collection of key nodes such as ENA members' residences, ENA-affiliated businesses, and important community centers.
    - **Area of Operations (AO):** The entire county. The goal is to develop a deep, holistic understanding of the county's political, social, and economic landscape to identify emerging threats to the ENA community's stability and security.
    - **Area of Interest (AI):** All adjacent counties, the state capital (where relevant laws are made), major metropolitan areas that exert economic or media influence on the AO, and the known operating areas of regional or national-level threat groups that have shown interest in the AO.
- **Mission: Protective Security for a Designated ENA Leader**
    - **Bullseye:** The designated ENA leader (the Principal).
    - **Area of Operations (AO):** The AO is dynamic and moves with the Principal. It includes their primary residence, their place of work, and the specific routes they travel between them. When the Principal is at a location, the AO encompasses the immediate area they are in and the surrounding space that must be controlled or monitored for their security.
    - **Area of Interest (AI):** The entire metropolitan or regional area in which the Principal lives and works. The AI must include the locations of all known potential threats, transportation hubs, hospitals, and safe locations. It also includes the online information environment, monitoring for specific threats or negative sentiment directed at the Principal. The AI expands or shifts based on the Principal's travel schedule.

2-5. Analyzing the Mission and ENA/SC Leader's Intent

The IPOE process is mission-driven. Therefore, a critical activity in Step 1 is to conduct a thorough analysis of the order or directive received from the higher ENA or SC command. This analysis, a core component of the adapted Troop Leading Procedures (SCDP 5-0, *Planning*), ensures our intelligence effort is precisely aligned with the leader's requirements. This involves identifying three types of tasks:

1. **Specified Tasks:** These are tasks that are explicitly stated in the order. They are the "must-do" items. For example, an order might state, "*1st Squad will provide security for the ENA Regional Assembly at the Liberty Hall.*" The specified task is clear.

2. **Implied Tasks:** These are tasks that are not explicitly stated in the order but are necessary to accomplish the specified tasks or the overall mission. The analyst must think critically to identify these. For the example above, implied tasks would include:

- *Conduct a physical reconnaissance of Liberty Hall (lawfully).*
- *Develop an access control plan.*
- *Establish observation posts to monitor approaches.*
- *Coordinate with ENA event organizers.*
- *Develop a lawful contingency plan for disruptions.*
- *Verify the legality of all planned security measures under local ordinances.*

  Identifying implied tasks is crucial for developing a complete and realistic plan.

3. **Essential Task:** This is the single, overarching task that must be accomplished to achieve the mission's purpose. It is the core of the mission. For the event security example, the essential task is: *Protect ENA members and ensure the assembly can proceed without unlawful disruption.* All other tasks, specified and implied, must support the accomplishment of this essential task.

By deconstructing the mission in this way, we identify the specific actions our element must be prepared to take. This analysis directly informs our IPOE by telling us what information we will need. To develop an access control plan, we need to know the layout of the building. To establish OPs, we need to analyze the surrounding terrain. To develop a contingency plan, we need to know the capabilities of potential threats. This task analysis transforms a broad directive into a focused set of preliminary intelligence questions.

2-6. Identifying Significant Characteristics of the Operational Environment

With the geographic boundaries defined and the mission requirements understood, the next activity is to conduct a broad, initial scan of the AO and AI to identify the most significant characteristics that are likely to influence the operation. This is not the deep, detailed analysis of Step 2; rather, it is a high-level survey designed to identify the "big rocks" that will demand our primary analytical attention. We use the PMESII-PT framework as our guide for this scan.

The analyst should ask, for each domain, "What are the one or two most important factors here that could affect this specific mission?"

- **(P) Political:** Is there a contentious local election approaching? Is there a controversial new law or ordinance being debated that is relevant to our mission?
- **(M) Military (LE):** Is the local law enforcement agency known to be professional and responsive, or are they understaffed and slow to react? Are there any known jurisdictional overlaps or rivalries?
- **(E) Economic:** Is the community economically stable, or are there major stressors like a recent factory closure that could contribute to social tension?
- **(S) Social:** Are there well-known and deep-seated tensions between different social, ethnic, or political groups in the AO? Are there any specific activist or extremist groups (left or right) known to be active in the area that might take an interest in our mission?
- **(I) Information:** Is there a dominant local media outlet with a strong and predictable bias? Are there influential online figures or forums that drive the local narrative?
- **(I) Infrastructure:** Is there a single, critical piece of infrastructure—like a bridge, tunnel, or power substation—whose failure would cripple the AO or our mission?
- **(P) Physical Environment:** Is the area prone to a specific type of severe weather (e.g., tornadoes, blizzards) that must be factored into planning? Is the topography dominated by

a single key terrain feature?
- **(T) Time:** Is the mission taking place on or near the anniversary of a significant or controversial historical event? Does it coincide with another major local event (e.g., a festival, a sports game) that will affect traffic and population density?

This initial scan creates a preliminary list of the most important environmental factors. It allows us to immediately prioritize our subsequent, more detailed analysis, ensuring we focus on the characteristics that pose the greatest threat or offer the greatest opportunity for our specific mission.

2-7. Identifying Intelligence Gaps and Initial Information Requirements

The final activity of Step 1 is to synthesize the work done so far into a set of focused questions that will drive the rest of the IPOE process. This involves a simple but critical intellectual exercise: comparing what we know with what we *need* to know to accomplish the mission lawfully and effectively.

The analyst should create a simple ledger:

- **What We Know:** List the established facts and solid baseline information gathered during the initial scan. (e.g., “We know the ENA meeting is at Liberty Hall on Saturday,” “We know from *The Area Study* that the Liberty County Minutemen and the Liberty Action Collective are both active in the AO.”)

- **What We Need to Know (Intelligence Gaps):** List the critical questions that remain unanswered. These gaps in our knowledge represent a risk to the mission. (e.g., “We do not know if either group is planning a protest or counter-protest at the event,” “We do not know the exact security protocols of the Liberty Hall venue,” “We do not know the precise legal requirements for establishing an access control point under city ordinance.”)

These intelligence gaps are then transformed into a prioritized list of **Information Needs**. An Information Need is a clear, focused question that the leader needs answered to make a decision or finalize a plan. They are the initial output that tasks the intelligence collection and analysis effort. Examples of initial Information Needs derived from the gaps above could be:

- **Priority 1:** What are the specific legal requirements and restrictions for private security at the Liberty Hall venue according to city and state law?
- **Priority 2:** What is the current disposition and stated intent of the Liberty County Minutemen and the Liberty Action Collective regarding the ENA meeting?
- **Priority 3:** What is the detailed physical layout of Liberty Hall and its immediate surroundings, including all entry/exit points, potential observation posts, and existing security features?

Formulating and prioritizing these Information Needs is the culminating activity of Step 1. It ensures that the detailed analytical work of the subsequent IPOE steps is purposeful and directly supports the leader’s decision-making process.

2-8. The Output of Step 1: The Foundation for Analysis

Upon completion of Step 1, the SC leader and their intelligence personnel should have produced

three essential products that form the foundation for the rest of the IPOE process:

1. **A Defined Operational Environment:** This includes a map or overlay clearly delineating the boundaries of the mission's Area of Operations (AO) and Area of Interest (AI).
2. **A List of Significant OE Characteristics:** A summary of the key PMESII-PT factors identified during the initial scan that are most likely to influence the operation.
3. **A Prioritized List of Initial Information Needs:** A set of focused questions that will guide the detailed collection and analysis efforts in Steps 2, 3, and 4.

2-9. Conclusion

Step 1 of the IPOE process is an act of intellectual discipline. It is the deliberate effort to impose focus, define boundaries, and ask the right questions before diving into detailed analysis. By systematically identifying our geographic limits, understanding our mission requirements, scanning the environment for its most significant features, and formulating clear Information Needs, we prevent the "analysis paralysis" that can plague an unfocused intelligence effort. This foundational step ensures that the work that follows is efficient, relevant, and directly contributory to the SC's ability to make sound, lawful decisions. With this clear direction established, we are now prepared to move to Step 2: the detailed work of describing how the specific characteristics of this defined environment will affect our operations.

Chapter 3: Step 2 - Describe Environmental Effects on Operations

3-1. Introduction

Having defined the operational environment in Step 1, we now move to the analytical core of the IPOE process: describing how the significant characteristics of that environment affect operations. The purpose of this step is to transform our initial list of environmental factors from a static collection of facts into a dynamic understanding of opportunities and constraints. The environment is not a passive backdrop; it is an active participant that shapes, channels, and influences the actions of every actor within it. A river is not merely a line on a map; it is an obstacle that canalizes movement and creates chokepoints. A local news station is not just a building; it is a powerful node that can shape public perception and incite or calm social tensions.

This chapter provides the methodology for analyzing these effects. We will dissect the two foundational domains upon which all human activity rests: the Physical Environment and the Information Environment. By systematically evaluating how the terrain, weather, media landscape, and communication networks impact both our own Security Corps elements and any potential threats, we build the essential context required for all subsequent analysis. The outputs of this step—overlays and matrices that visually and textually describe these environmental effects—are not academic exercises. They are the practical tools that allow us to visualize the battlefield, anticipate challenges, and develop plans that are grounded in the unforgiving realities of the operational environment.

3-2. The Physical Environment (Terrain & Weather)

The physical environment is the most permanent and fundamental variable in any operation. It is the stage upon which all actions unfold. Weather and terrain dictate where forces can move, what they can see, where they can find protection, and how effective their equipment will be. A leader who fails to respect the physical environment is doomed to fail, regardless of their own strength or the weakness of their opponent. Our goal is to analyze this domain with such rigor that we can see the landscape not just as a resident, but as a strategist, identifying its opportunities and limitations for both our protective mission and for any potential threat.

3-3. Terrain Analysis (OAKOC/KOCOA)

The Security Corps adapts the time-tested military framework for terrain analysis, OAKOC (Observation and Fields of Fire, Avenues of Approach, Key Terrain, Obstacles, and Cover and Concealment), to our specific protective mission. This framework provides a systematic way to dissect the strategic implications of the physical landscape.

a. Observation and Fields of Fire

- **Definition: Observation** is the ability to see the surrounding area from a specific vantage point, either with the naked eye or with optics. **Fields of Fire** are the areas that a weapon can effectively cover from a given position. For the SC, this analysis is crucial for establishing security. Good observation provides early warning of approaching threats,

while good fields of fire are essential for establishing a lawful defensive posture to protect a person or place.

- **Analysis:** To analyze observation, you must identify the locations that offer a commanding view of your Area of Operations. This is not limited to hilltops; it can include tall buildings, highway overpasses, or even long, straight stretches of open road. Use topographic maps (from sources like the USGS) to identify high ground. Use digital tools like Google Earth Pro to tilt the view and visualize lines of sight from any point. Critically, you must also identify "dead space"—areas that cannot be seen from a given observation post due to terrain masking or obstructions.
- **SC Application:** This analysis directly informs the placement of lawful **Observation Posts (OPs)** for event security or community monitoring. It helps you understand the vulnerabilities of your own locations—who can see your home or facility? It also allows you to predict where a potential threat might position themselves to conduct surveillance on your activities. When planning a defensive posture, analyzing fields of fire is a non-negotiable legal and tactical requirement. You must ensure that your positions can lawfully and effectively cover the most likely avenues of approach to the asset you are protecting, while simultaneously understanding where your fields of fire are limited.

b. Avenues of Approach

- **Definition:** An **Avenue of Approach (AA)** is any route, by air or land, that a force can use to reach an objective or key terrain. AAs are comprised of one or more **Mobility Corridors**—areas where movement is channeled by restrictive terrain.
- **Analysis:** The first step is to identify all mobility corridors using your analysis of obstacles. On a map, look for the paths of least resistance between major obstacles. These are the natural channels for movement. Group these corridors to form Avenues of Approach. AAs exist for vehicle traffic (roads, flat open ground), foot traffic (trails, sidewalks, wooded paths), and even for Unmanned Systems (UxS) (valleys, areas clear of obstructions).
- **SC Application:** A thorough analysis of AAs is the foundation of all movement planning. It is how you develop your P.A.C.E. (Primary, Alternate, Contingency, Emergency) routes for a potential evacuation. By understanding the AAs, you can predict the most likely routes that evacuating civilians, responding authorities, or an approaching threat will use. This knowledge allows you to position your own security elements to monitor these routes, avoid chokepoints, and anticipate where contact or conflict is most likely to occur.

c. Key Terrain

- **Definition: Key Terrain** is any locality or area whose seizure, retention, or control affords a *marked advantage* to either side. This is one of the most important concepts in terrain analysis. A piece of terrain is not key simply because it is high or useful; it is key because its control is decisive.
- **Analysis:** To identify key terrain, look for the features that have a disproportionate impact on operations within your AO. A bridge that is the only crossing over a major river is key terrain. The mountain pass that contains the only road through a region is key

terrain. The cell phone tower on the highest hill that provides communications for the entire county is key terrain. A major highway intersection that controls all north-south and east-west traffic is key terrain.

- **SC Application:** Identifying key terrain allows the SC to prioritize its limited resources. During a community stability monitoring mission, key terrain features are the locations you must monitor to understand the health of the entire system. For a security mission, key terrain features are the points you must lawfully control or influence to ensure the safety of your asset. It also tells you where a sophisticated adversary will focus their efforts. A threat seeking to disrupt the community will not attack a random street; they will target the key terrain—the bridge, the power substation, the intersection—to achieve the greatest effect with the least effort.

d. Obstacles

- **Definition:** An **obstacle** is any natural or man-made feature that slows, channels, fixes, or blocks movement. Obstacles dictate where and how forces can maneuver.
  - **Natural Obstacles:** Rivers, dense forests, swamps, steep ravines, and significant rock fields.
  - **Man-made Obstacles:** High concrete walls, railroad embankments, dense urban areas, and deliberately emplaced barriers.
- **Analysis:** Using maps, satellite imagery, and physical reconnaissance, catalog all major obstacles in your AO. Note their characteristics. Is the river fordable? How dense is the forest? How high is the wall? Your analysis should classify terrain based on its effect on movement (e.g., for vehicles, is it unrestricted, restricted, or severely restricted?).
- **SC Application:** A detailed understanding of obstacles is critical for all route planning. It reveals the mobility corridors and AAs. It also informs your defensive planning; a good defensive position always ties into existing obstacles to limit an attacker's options. Furthermore, understanding obstacles allows you to predict where an adversary will be canalized, making them vulnerable to lawful observation or defensive action.

e. Cover and Concealment

- **Definition:** These two terms are not interchangeable, and the distinction is critical for survival. **Cover** is protection from the effects of fires (e.g., bullets, shrapnel). It is something that will physically stop projectiles, like a thick stone wall, a large earth berm, or a deep ditch. **Concealment** is protection from observation, but it will *not* stop projectiles. It is something that can hide you, like tall grass, thick bushes, or a smoke screen.
- **Analysis:** Map the areas in your AO that offer good cover and concealment. A dense forest offers excellent concealment but almost no cover from anything larger than a small caliber round. A concrete highway divider offers excellent cover but little concealment. A building can offer both, depending on its construction.
- **SC Application:** This analysis is fundamental to all tactical-level actions. When planning a movement route, you must seek paths that offer both cover and concealment where possible. When establishing an OP, concealment is your primary concern. When selecting

a position for a lawful defensive action, cover is paramount. This analysis also helps you identify likely ambush sites that a potential threat might use—locations that offer both good concealment for them and limited cover for their target.

3-4. Weather Analysis

Weather is a pervasive and impartial factor that can have a profound impact on every aspect of an operation. A plan that does not account for the weather is incomplete and irresponsible. We must analyze both the long-term climate patterns and the short-term weather forecast.

- **Visibility:** How far can we see? This is affected by the time of day, moon phase (illumination), and atmospheric conditions like fog, rain, snow, or dust. Poor visibility can aid a force seeking to move undetected (good for OPSEC), but it severely hampers observation and the ability to identify threats at a distance. It also impacts the effectiveness of optics and some sensors.
- **Wind:** Wind speed and direction are critical. High winds can make UxS operations unsafe or impossible. Wind direction dictates the spread of smoke (whether for concealment or from a fire) and any potential Chemical, Biological, Radiological, or Nuclear (CBRN) hazards. It can also carry sound, affecting noise discipline.
- **Precipitation:** Rain, snow, sleet, or hail affects mobility, visibility, and morale. Heavy rain can turn roads to mud and cause flash floods, rendering some AAs impassable. Snow and ice create obvious mobility challenges. Precipitation also degrades the performance of some communications equipment and optics and can make it harder to maintain personal readiness.
- **Temperature and Humidity:** Extreme heat or cold has a direct and significant impact on the physical performance and morale of personnel. It requires specific planning for hydration, clothing, and work/rest cycles. Extreme temperatures also affect equipment performance, particularly battery life, which is a critical consideration for SC communications and electronics. High humidity can exacerbate the effects of heat and increase equipment maintenance requirements.

3-5. Synthesizing the Physical Environment: The MCOO and Effects Matrices

The raw analysis of OAKOC and weather must be synthesized into usable products that clearly communicate the environment’s effects to the leader and the entire element.

- **The Modified Combined Obstacle Overlay (MCOO):** The MCOO is the primary graphic product for synthesizing terrain analysis. It is a map overlay that visually depicts all militarily significant aspects of the terrain. A simplified MCOO for SC use should clearly show:

Avenues of Approach: The major vehicle and foot routes identified in your analysis, depicted with arrows.
Key Terrain: Clearly circled and marked with a ‘K’.
Obstacles: Major natural and man-made obstacles.

Terrain Mobility Classifications: The entire map should be color-coded or shaded to show areas of unrestricted, restricted, and severely restricted terrain.

The MCOO provides an at-a-glance picture of the physical "battlefield," allowing a leader to instantly see how the terrain channels movement and where the decisive points are located.

- **The Terrain Effects Matrix:** This is a simple table that accompanies the MCOO. It provides a concise written summary of the OAKOC analysis and its implications. It answers the "So what?" for the terrain.

OAKOC Factor	Effects on SC & Threat Operations
Observation	High ground on Patriot's Ridge provides excellent observation over the primary AA (I-76). Threat surveillance OPs are likely here. SC OPs should be placed on the eastern hills to observe Patriot's Ridge itself.
Avenues of App.	I-76 is the primary vehicle AA but will be a major chokepoint. The western farm roads provide a viable alternate AA for smaller vehicles. Threats will likely use wooded trails for dismounted infiltration.
Key Terrain	The Miller Bridge is key terrain; its control is decisive for all north-south movement in the AO. The cell tower on Patriot's Ridge is key terrain for communications.
Obstacles	The Freedom River is a major obstacle, canalizing all traffic to the two bridges. The swamps in the south are severely restricted terrain for all vehicles.
Cover/Conceal.	Dense forests in the west offer excellent concealment but poor cover. The industrial park in the south offers good cover from its concrete buildings.

- **The Weather Effects Matrix:** This matrix summarizes the anticipated effects of the weather forecast on specific SC and threat capabilities.

Weather Element	Effect on SC Operations	Effect on Threat Operations
Forecast: Heavy Rain	Vehicle mobility on secondary roads will be degraded. Visibility will be reduced to <500m, hampering OPs. Rain will help mask noise of movement.	Same mobility/visibility effects. Will allow for easier concealed infiltration under cover of weather.
Forecast: High Winds	UxS operations will be suspended. Radio communications may be degraded due to wind noise.	Same UxS limitations. May use wind to mask noise of their own approach.

3-6. The Information Environment

The information environment is the "human terrain" of knowledge, belief, and perception. It is the nervous system of a community. In modern conflicts and crises, the battle for narrative control is often as important as control of physical terrain. Understanding this environment allows the SC to anticipate public reactions, counter hostile propaganda, and communicate its own lawful purpose effectively.

3-7. The Media Landscape

- **Analysis:** Identify the dominant formal media outlets that cover your AO. This includes local television news affiliates, major AM/FM news and talk radio stations, and the primary local and regional newspapers (both print and digital). The analysis must go beyond simple identification. You must assess each outlet's general political leaning, its level of credibility with the local population, and its typical narrative focus. Does a particular outlet favor sensationalism? Does another have a history of solid, fact-based reporting?
- **SC Application:** This assessment allows you to predict how your actions (or the actions of a threat) are likely to be reported. It helps you identify which outlets might be sympathetic, which might be hostile, and which are most influential. This knowledge is critical for planning any interaction with the media (which should always be coordinated through ENA channels) and for understanding the sources of information that are shaping the perceptions of the community you are sworn to protect.

3-8. Formal and Informal Networks

- **Analysis:** Information flows through both official and unofficial channels. **Formal networks** are how authorities communicate with the public. Identify these channels: the county emergency management agency's website and social media feeds, the sheriff's office alert system, etc. **Informal networks** (the "grapevine") are how people *really* talk to each other. This includes the physical nodes like the local coffee shop, barbershop, or gun store, and the digital nodes like the main town Facebook group or a Nextdoor forum.
- **SC Application:** Knowing the formal networks is essential for receiving official instructions and warnings during a crisis. Monitoring the informal networks (lawfully and passively) is the single best way to take the real-time pulse of the community. It allows you to identify emerging concerns, track the spread of rumors, and understand the "word on the street," which often moves faster and has more influence than official news. It is a critical source of early warning for social instability.

3-9. The Online Environment

- **Analysis:** Much of modern radicalization, organization, and mobilization occurs online. This analysis focuses on identifying the specific digital platforms used by the ENA community and any potential threat groups you have identified. What specific websites, social media platforms (e.g., Facebook, X, Telegram, Gab), or online forums do they use for propaganda, recruitment, and planning? What are the key narratives, themes, and conspiracy theories they are pushing?
- **SC Application:** Lawful, passive monitoring of these public online spaces is a primary source of intelligence and early warning for the SC. It allows you to understand the ideology, intent, and capabilities of potential threat groups. It can provide specific warnings of planned protests, counter-protests, or other direct actions. **CRITICAL NOTE:** This activity must be conducted with the strictest adherence to legal and OPSEC principles. Do not engage, infiltrate, or make contact. Use accounts that are not tied to

your personal identity. Your role is solely that of a passive collector of publicly available information.

3-10. Synthesizing the Information Environment

The output of this analysis is a **Combined Information Overlay (CIO)** or a written assessment. Unlike the MCOO, the CIO is less of a literal map overlay and more of a conceptual diagram or summary. It should identify the key media players and their biases, map the flow of formal and informal information, and list the key online hubs for relevant groups. This product gives the SC leader a map of the "informational terrain," allowing them to navigate it as skillfully as they navigate the physical terrain.

3-11. Conclusion

The successful completion of Step 2 marks a critical transition in the IPOE process. We have moved beyond merely defining our area of concern to achieving a deep, multi-domain understanding of how that environment actually functions. We have created the foundational analytical products—the MCOO, the effects matrices, and the information environment assessment—that describe the opportunities and constraints imposed by the physical world and the world of ideas. We have built the stage and analyzed its properties in detail. With this essential context established, we are now fully prepared to move to Step 3: to place our detailed models of potential threats onto this stage and begin the work of evaluating their capabilities and intentions.

Chapter 4: Step 2 (Continued) - Describe Environmental Effects on Operations (The Human Domain)

4-1. Introduction

Having analyzed the foundational physical and information domains, we now turn our attention to the most complex, dynamic, and often decisive element of any operational environment: the human domain. While terrain sets the stage and information shapes perception, it is the people—their social structures, political systems, and economic realities—who drive the action. A river or a radio tower behaves in predictable ways; human beings, influenced by culture, belief, fear, and interest, are infinitely more complex.

The purpose of this chapter is to continue the work of Step 2 by providing a methodology for analyzing this human domain. A failure to understand the people within our Area of Operations (AO) is a failure to understand the mission itself. It is a critical vulnerability that can lead to flawed assumptions, alienated communities, and ultimately, the failure to provide effective, lawful protection. We will deconstruct this domain using the relevant components of the PMESII-PT framework: the Social, Political, and Economic environments. Our goal is to move beyond a superficial understanding and develop a deep, functional model of the society in which we operate, identifying its sources of strength, its hidden fault lines, its key influencers, and its potential for instability. This analysis is not an academic exercise in sociology; it is a fundamental intelligence task essential for the survival and success of the Security Corps.

4-2. The Social Environment: The Fabric of the Community

The social environment encompasses the people, their culture, and the groups they form. It is the living fabric of the community. Understanding this fabric—its texture, its strengths, and its tears—is essential for any SC operation, as it dictates how people will react to a crisis, who they will trust, and where conflicts are most likely to erupt.

a. Demographics: The Statistical Foundation

Before we can understand a population's character, we must understand its composition. Demographics provide the objective, statistical baseline for our social analysis—the "who, what, where, and how many" of our AO.

- **Analysis:** Using authoritative sources like the U.S. Census Bureau (data.census.gov) and local government planning departments, we must collect and analyze key demographic data for our AO. This includes:
    - **Population Density and Distribution:** Where do people live? Are they concentrated in a dense urban core, spread out in suburbs, or scattered across a rural landscape? A population density map is a foundational IPOE product.
    - **Age:** What is the median age? A community with a high percentage of elderly or very young residents (a high dependency ratio) will have different needs and vulnerabilities during a crisis, particularly regarding mobility and medical care.
    - **Ethnicity and Race:** What is the ethnic and racial makeup of the community? Are there distinct, concentrated ethnic enclaves? Understanding this is key to cultural

awareness and identifying potential social fault lines.
    - **Income and Poverty Levels:** What is the median household income and the poverty rate? High poverty and economic disparity can be significant drivers of social stress, crime, and susceptibility to extremist ideologies.
- **SC Application:** This hard data is a powerful analytical tool. By overlaying a population density map with our flood zone map (from Chapter 3), we can immediately quantify the number of people at risk in a natural disaster. By understanding the location of elderly communities, we can anticipate areas that will require priority assistance in a power outage. Demographics provide the essential, factual starting point for all deeper social analysis.

b. Culture and Religion: The Unwritten Rules

If demographics are the "what," culture is the "why." Culture encompasses the shared beliefs, values, customs, and behaviors that define a community. Religion is often a central pillar of culture, providing a moral framework, a powerful community network, and physical centers of gravity.

- **Analysis:** The analyst must identify the dominant cultural norms and religious institutions in the AO. What are the major faiths practiced? Where are the largest and most influential churches, mosques, synagogues, or temples located? These buildings are more than just places of worship; in a crisis, they often become de facto shelters, communication hubs, and aid distribution points because they have established, trusted networks. What are the unwritten rules of the community? Is it generally conservative or liberal? Is there a strong identity tied to a specific industry or heritage?
- **SC Application:** Understanding the cultural and religious landscape allows us to operate with respect and effectiveness. It helps us communicate in a way that will be understood and accepted. It allows us to anticipate which institutions will become influential during a crisis. Knowing that a particular church has a large, active, and well-organized congregation is a critical piece of intelligence; in an emergency, that church is likely to be a major player in the local response, a potential partner for lawful coordination, and a key source of information.

c. Social Cohesion and Division: The Fault Lines and Power Brokers

No community is a monolith. Every society has forces that bind it together and fault lines that threaten to pull it apart. One of the most important analytical tasks in the IPOE process is to identify these sources of cohesion and division.

- **Analysis:** We must map the key **sources of cohesion**—the formal and informal groups that represent a reservoir of organized, civic-minded volunteers. This includes civic clubs (Rotary, Lions), veterans' posts (VFW, American Legion), major non-profits, and volunteer fire departments. Equally important is the identification of **social fault lines**—the divisions within a society that can be a source of tension or conflict. These can be based on economics (rich vs. poor), politics (sharp partisan divides), race/ethnicity, or culture (e.g., long-time rural residents vs. new suburban arrivals). The analyst must listen to the community's discourse by attending public meetings (like city council or school board meetings) and lawfully monitoring local news editorials and online forums to

identify these key issues.

- **SC Application:** This analysis provides a dynamic map of the social landscape. It tells us which groups are likely to cooperate in a crisis and which are likely to come into conflict. It allows us to predict where instability is most likely to arise under stress. For example, a heated zoning dispute between farmers and developers is a fault line that could escalate into protests or direct action. This predictive understanding is vital for any mission focused on maintaining community stability.

d. Ideological Group Mapping

This is a critical and sensitive subset of social analysis that must be conducted with the utmost objectivity and discipline. As stated in *The Area Study*, our role is that of a dispassionate intelligence collector cataloging potential threats to civil order, not a political commentator. The goal is to objectively identify and understand any politically or ideologically motivated groups across the spectrum that have a presence in our AO/AI and possess the potential to cause significant disruption, engage in violence, or damage infrastructure.

- **Objective Identification:** Our focus is on observable behavior and publicly stated goals. We must catalog groups from all sides of the ideological spectrum whose tactics or ideology could pose a security concern.
    - **Left-Wing Groups:** This category can include a range of organizations, such as revolutionary Marxist groups, socialist alternative organizations, and anarchist or anti-fascist (Antifa) networks. Our collection must focus on:
        - **Stated Goals:** What are their public objectives (e.g., anti-capitalism, abolition of police)?
        - **Typical Tactics:** How do they typically operate? (e.g., public protests, organized marches, counter-protesting right-wing events, property damage, physical confrontations).
        - **Areas of Operation:** In which parts of our AO/AI are they most active (e.g., urban centers, university campuses)?
    - **Right-Wing Groups:** This category can include a range of organizations, such as militias (often focused on anti-government sentiment), sovereign citizen movements, and white supremacist or neo-Nazi organizations. Our collection must focus on:
        - **Stated Goals:** What are their public objectives (e.g., defending the Constitution, preparing for societal collapse, preserving a specific ethnic identity)?
        - **Typical Activities:** How do they typically operate? (e.g., public rallies, recruitment drives, operating compounds, paramilitary-style training).
        - **Areas of Operation:** In which parts of our AO/AI are they known to be active (e.g., rural areas, specific towns)?
- **Lawful Collection and Analysis:** Data on these groups must be collected from credible, open sources. Start with reports from professional monitoring organizations (like the ADL and SPLC), academic institutions, and law enforcement bulletins. Cross-reference this with local news archives to find reports of their specific activities within your AO. Lawfully and passively monitor their own public websites and social media to understand their self-perception and propaganda. **CRITICAL SAFETY NOTE: At no time will SC members attempt to infiltrate, make contact with, or engage with these groups for**

intelligence purposes. Our role is strictly that of a passive, open-source analyst. Maintain rigorous personal operational security.

- **SC Application:** The output of this analysis is an objective fact sheet for each identified group, detailing their ideology, leadership (if known), estimated presence in the AO, and a summary of their past activities. This is not a political judgment; it is a threat assessment. It allows us to anticipate potential flashpoints, plan security for ENA events that might draw their attention, and develop evacuation routes that avoid their known operating areas during times of civil unrest.

4-3. The Political Environment: The Structures of Power

The political environment is the system of rules and rulers that governs public life. In a crisis, the decisions made by political leaders will directly affect our freedom of movement, our access to resources, and our personal security. We must know who is in charge, the extent of their power, and the legal framework within which they—and we—operate.

a. Formal Governance

- **Analysis:** We must map the official chain of command. This involves identifying the key political jurisdictions (city, county, state legislative districts) and the **key elected officials** who govern them: Mayor, City Council, County Commissioners, Sheriff, District Attorney, and our specific State Representatives. For each official, we must note their political party and, more importantly, their general political stances and key allies as revealed through local news analysis and public records.
- **SC Application:** This “political order of battle” tells us who the decision-makers are. Knowing that the County Sheriff has a strong “law and order” stance while the Mayor is more focused on de-escalation allows us to predict how a civil disturbance might be handled differently depending on the jurisdiction. It tells us who to lawfully monitor for official declarations and instructions during an emergency.

b. Informal Power Structures

- **Analysis:** Official titles do not tell the whole story. We must also identify the **informal power brokers**—individuals or groups who wield significant influence without holding office. This could be a wealthy family that heavily funds local campaigns, a powerful labor union, the local Chamber of Commerce, or an influential pastor. Their influence can be mapped by tracking campaign donations (often public record), reviewing the boards of major local charities and institutions, and paying attention to who is consistently quoted in the local paper on key issues.
- **SC Application:** Understanding the informal power structure reveals the hidden lines of influence. In a crisis, these informal leaders can often mobilize resources or shape community opinion faster than formal government. Knowing who they are provides a more complete picture of the political landscape and identifies other key individuals to monitor for indicators of community response.

c. The Legal Framework

- **Analysis:** This is a non-negotiable intelligence requirement. We must research and summarize the key state and local laws that govern our potential actions. This includes:
    - **Emergency Powers:** Who has the authority to declare a State of Emergency, and what specific powers does that grant them (e.g., curfews, travel restrictions, confiscation of property)?
    - **Use of Force and Self-Defense:** What are the specific state laws concerning self-defense (e.g., Castle Doctrine, Stand Your Ground)?
    - **Firearms Laws:** What are the state and local regulations on the possession, transport, and carrying of firearms?
    - **Surveillance and Privacy:** What are the state laws regarding video and audio recording of individuals?
    - **Assembly and Protest:** What are the local ordinances regarding public gatherings and what constitutes an unlawful assembly?
- **SC Application:** This knowledge defines our "legal terrain." It provides the absolute "left and right limits" for all SC planning and action. A plan that violates this framework is unlawful and therefore invalid. A summary of this legal framework is a critical component of the IPOE product and a mandatory briefing item for any operation.

4-4. The Economic Environment: The Flow of Resources

The economy is the circulatory system of a community. Its health dictates social stability, and its infrastructure dictates the flow of essential goods. A resilient community requires a resilient economy.

a. Economic Drivers

- **Analysis:** Identify the primary industries and the single largest employers in the AO. Is the area a "company town," critically dependent on one factory or business? Or does it have a diverse economic base? This information is readily available from the local Chamber of Commerce and county economic development offices.
- **SC Application:** This analysis reveals a key vulnerability. A community heavily dependent on a single employer is fragile; a strike or closure can lead to mass unemployment and rapid social destabilization, a critical indicator for the SC to monitor.

b. Logistics and Supply Chain

- **Analysis:** This is one of the most critical areas of study for preparedness. We must map the "just-in-time" logistics system that supplies our AO. This involves identifying the locations of major **food and retail distribution centers** that service our local stores, as well as the key transportation arteries (interstates, rail lines) that connect them.
- **SC Application:** This analysis reveals the fragility of our modern supply system. Knowing that all local grocery stores are serviced by a single distribution center 100 miles away tells us that a disruption on the connecting interstate will result in empty shelves within 2-3 days. This intelligence is the primary justification for personal and community stockpiling and for developing plans that account for supply chain failure.

c. Economic Vulnerabilities

- **Analysis:** Synthesize the analysis of economic drivers and logistics to identify the key points of failure. Is the community dependent on a single industry? Is it susceptible to supply chain disruption? Is there a significant black or grey market economy, indicating underlying economic stress but also an alternative network for goods?
- **SC Application:** This assessment allows us to develop realistic contingency plans. If we know the primary economic vulnerability is a supply chain disruption, our support plans can focus on facilitating local resource sharing and security for alternative food sources. If the vulnerability is the potential for mass layoffs, our monitoring can focus on indicators of social unrest.

4-5. The Output: A Multi-Layered Understanding of the Human Terrain

The culmination of the analysis described in this chapter is a deep, multi-layered understanding of the human domain. This understanding is captured in several key products that will be integrated into the final IPOE:

- **A Civil Considerations Assessment:** A written summary and potentially a map overlay that identifies key demographic concentrations, cultural and religious centers, social fault lines, and the locations of critical political and economic infrastructure.
- **Social Network Diagrams:** Simple link diagrams that visually map the relationships between key formal and informal leaders, influential groups, and potential threat actors.
- **Threat Group Fact Sheets:** Objective summaries for each identified ideological group, detailing their ideology, capabilities, and past activities in the AO.

4-6. Conclusion

The detailed analysis of the human domain is arguably the most challenging but also the most vital part of describing the environmental effects on our operations. We have moved from the static world of terrain and infrastructure to the dynamic and unpredictable world of people, power, and resources. We have now populated the stage we built in the previous chapter. We have a statistical baseline of the population, an understanding of its culture and fault lines, an objective assessment of potential threat groups, and a map of the political and economic systems that govern it. With this comprehensive, multi-domain picture of the human terrain complete, we are now fully prepared to move to Step 3: to evaluate these potential threats in detail and begin building predictive models of their behavior.

PART TWO: THREAT ANALYSIS AND OPERATIONAL APPLICATION

Chapter 5: Step 3 - Evaluate the Threat

5-1. Introduction

Having defined our operational environment and described its complex effects, we now pivot from analyzing the stage to analyzing the actors. The purpose of Step 3 of the IPOE process is to develop a deep, objective, and detailed understanding of the potential threats that may operate within that environment. This step is critical because a plan based on a generic or misunderstood adversary is a plan destined for failure. We must understand our potential adversaries not as we imagine them to be, or as their propaganda portrays them, but as they actually are: their organizational structure, their real-world capabilities, their preferred methods of operation, and their critical vulnerabilities.

This evaluation is conducted *independent* of the specific environmental effects analyzed in Step 2. The goal here is to build a baseline model of the threat in a vacuum—how they would prefer to operate under ideal conditions. This "doctrinal" understanding is essential because it reveals their core TTPs (Tactics, Techniques, and Procedures) and operational mindset. Only after we have built this baseline model can we, in Step 4, place the threat back into the specific environment of our AO to predict their actual Courses of Action (COAs). This chapter provides the methodology for deconstructing any potential threat, from a loosely organized activist network to a sophisticated criminal element, and building the detailed Threat Models that are the cornerstone of predictive intelligence.

5-2. Defining "Threat" in the SC Context

For the Security Corps, a **threat** is any individual, group, or condition that has the *capability* and *intent* to harm the Euramerican national community, undermine ENA interests, disrupt lawful SC operations, or otherwise threaten the safety and stability we are sworn to protect. This is a broad definition that requires careful, objective analysis. A group that disagrees with the ENA politically but operates peacefully and lawfully is not a threat; they are a political opponent. A group, however, that uses or credibly threatens violence, property damage, or significant unlawful disruption to achieve its ideological goals is a threat that must be evaluated. Our focus is always on observable behavior and capability, not political labels.

5-3. Identifying Threat Characteristics

The first activity in evaluating a threat is to systematically catalog its key characteristics. This process, adapted from the military concept of Order of Battle, provides a structured way to deconstruct a threat organization and understand its components. We must analyze each potential threat actor identified in Step 1 through this lens.

a. Composition and Disposition

- **Composition:** This describes the threat's organizational structure and equipment. How are they organized? Is there a clear hierarchy with identifiable leaders, or are they a decentralized network of autonomous cells? What is their command and control (C2) mechanism—do they use encrypted apps, social media, or face-to-face meetings? What

equipment do they possess? This includes not just weapons (and their legal status), but also communications gear, vehicles, protective equipment, and any specialized tools (e.g., for breaching or creating obstacles).

- **Disposition:** This describes how the threat is geographically arrayed. Where are their known or suspected meeting places, training areas, or safe houses? Do they have a physical headquarters or are they dispersed throughout the community? Do they concentrate their presence in urban or rural areas?
- **SC Application:** Understanding composition and disposition allows us to build a "political order of battle." It tells us who the key leaders are that we need to monitor (lawfully, via open sources), what their C2 methods are so we can understand their potential for rapid mobilization, and where they are located so we can plan our own activities to avoid or lawfully monitor them.

b. Strength and Combat Effectiveness

- **Strength:** This is a quantitative assessment. What is the threat's estimated number of members or active supporters in our AO/AI? How many vehicles or key pieces of equipment can they field? This information is often difficult to obtain and must be estimated from open sources (e.g., rally attendance, online membership numbers), always noting the low confidence of such estimates.
- **Combat Effectiveness:** This is a qualitative assessment of their ability to actually perform their stated mission. It is a measure of their fighting quality and resilience. Factors to consider include:
  - **Training:** Do they conduct organized training? Is it realistic paramilitary-style training, or is it limited to protest marshalling?
  - **Experience:** Do their members have prior military or law enforcement experience? Have they participated in past violent confrontations?
  - **Leadership:** Is their leadership experienced, charismatic, and respected, or are they disorganized and prone to infighting?
  - **Morale and Discipline:** Are their members highly motivated and disciplined, or are they an unruly mob? Do they have a history of maintaining cohesion under pressure?
- **SC Application:** A group of 100 poorly trained, undisciplined individuals may pose less of a threat than a group of 10 highly trained, experienced, and motivated individuals. This analysis allows us to move beyond simple numbers and assess the threat's actual capability to cause harm or disruption, which is essential for a realistic risk assessment.

c. Doctrine and Tactics (Observed TTPs)

- **Doctrine:** This refers to the threat's fundamental principles and beliefs that guide their actions. What is their core ideology? What do they consider a "win"? Do they follow the teachings of a particular political theorist or revolutionary?
- **Tactics (TTPs):** This is how they translate their doctrine into action. Based on historical analysis of their past activities (from news reports and other open sources), what are their preferred TTPs?
  - For a protest group, this could include: forming human chains, using "de-arresting"

tactics, employing shields and helmets, targeting specific infrastructure, or using social media to swarm a location.
    - For a militia group, this could include: establishing vehicle checkpoints, conducting armed patrols, using specific movement formations, or setting up security perimeters.
- **SC Application:** This is perhaps the most critical part of the evaluation. By understanding a threat's TTPs, we can predict *how* they will act in a given situation. If we know a group's preferred tactic for disrupting an event is to block the main entrance, our security plan can prioritize that location. If we know a group uses specific online platforms to organize, we can lawfully monitor those platforms for early warning. Understanding their TTPs allows for truly predictive, rather than reactive, security planning.

d. Support and Relationships

- **Analysis:** No threat operates in a complete vacuum. We must identify their support systems and key relationships.
    - **Logistics:** How do they sustain themselves? What are their sources of funding? Do they have a supply system for equipment, food, or medical supplies?
    - **Recruitment:** How do they attract and vet new members? Do they use online platforms, public events, or personal networks?
    - **Relationships:** Do they have alliances or rivalries with other groups in the AO? Do they have any known political patrons or sympathetic media contacts? Are they part of a larger national or transnational network?
- **SC Application:** Analyzing these factors reveals critical vulnerabilities and capabilities. A group with a sophisticated funding network is more resilient than one that relies on small donations. A group that is part of a national network can potentially call on outside support, increasing their strength rapidly. Identifying these support systems and relationships provides a more complete picture of the threat's resilience and reach.

5-4. Creating Threat Models

The culmination of our analysis of threat characteristics is the creation of a **Threat Model** for each significant potential adversary. A Threat Model is an analytical tool that synthesizes our understanding of a threat into a simple, usable format. It allows us to codify our knowledge and provides the essential baseline for Step 4. A complete SC Threat Model has three components.

a. The Doctrinal Template (Graphic)

- **Purpose:** The doctrinal template is a simple graphic that illustrates how a threat *prefers* to organize and deploy its forces and capabilities to conduct a specific type of operation, unconstrained by the environment. It is a picture of their "textbook" solution to a tactical problem.
- **Creation:** Based on our analysis of the threat's composition and observed TTPs, we can create simple templates for their most common actions. These are not complex military graphics, but simple sketches or diagrams.
    - **Example 1: Template for an Activist Group's Road Blockade.** The template might show a line of protestors forming a human chain across a road, with a second line of

"shield bearers" behind them. It would show a "medic" station set up on a nearby sidewalk and "scouts" positioned at either end of the block to provide early warning of law enforcement arrival.
    - **Example 2: Template for a Militia's "Show of Force" Patrol.** The template might show a small group moving in a specific tactical formation (e.g., a wedge), with designated roles for point man, rear security, and a team leader.
    - **Example 3: Template for a Routine Police Response to a Protest.** The template could show a line of patrol cars establishing a perimeter, with a designated command post vehicle and staging areas for additional officers.
- **Value:** These templates provide a visual baseline. They are a hypothesis of how the threat will act. In Step 4, we will take this "ideal" template and overlay it onto the actual terrain of our AO to see how the environment forces them to deviate, allowing us to predict their actual dispositions.

b. Description of Tactics and Options

- **Purpose:** This is a concise narrative that accompanies the graphic template. It adds the essential detail and context that a simple graphic cannot convey.
- **Content:** The narrative should describe:
    - **The Threat's Objective:** What is the group trying to achieve with this specific action (e.g., "Objective is to shut down traffic on the Miller Bridge for maximum media exposure.")?
    - **Key Tasks:** What are the essential functions that different parts of the group perform (e.g., "The scout element provides early warning," "The shield line engages law enforcement," "The media team live-streams the event.")?
    - **Branches and Sequels:** This is a critical analytical element. What are the threat's likely options if their initial action succeeds or fails?
        - **Branches (Contingencies):** What will they do if confronted? (e.g., "If law enforcement gives a dispersal order, Branch 1 is to comply and move to the secondary protest point at the courthouse.")
        - **Sequels (Follow-on Actions):** What will they do if they succeed? (e.g., "If the blockade holds for one hour, Sequel 1 is to declare victory and disperse before mass arrests can be made.")
    - **Peculiarities:** Does this threat have any known unique characteristics? (e.g., "This group is known for its strict adherence to non-violence," or "This group has a history of targeting journalists," or "Their leader is known to be highly impulsive.")
- **Value:** This narrative provides a dynamic understanding of the threat. It moves beyond a static picture and helps us think through the likely flow of events, including the threat's own decision-making process.

c. Identifying High-Value Targets (HVTs)

- **Purpose:** A **High-Value Target (HVT)** is an asset that the threat commander requires for the successful completion of their mission. Identifying a threat's HVTs is a crucial analytical task because it reveals their critical vulnerabilities.
- **Analysis:** To identify a threat's HVTs, we must look at their operation from *their*

perspective. What is the one thing they cannot afford to lose? The HVT is not always a person. It can be:

- **A Key Leader:** The one individual who provides the charisma, direction, and C2 for the entire group.
- **A Key Piece of Equipment:** A communications van that serves as their C2 node, or a specific vehicle used for transport.
- **A Critical Resource:** A reliable funding source, or a sympathetic property owner who allows them to use their land for training.
- **A Key Information Asset:** A specific social media account or website that is their primary tool for recruitment and mobilization.
- **A Belief or Idea:** Their perceived legitimacy with the community, or their public image of being "defenders of the people."

- **SC Application:** We identify a threat's HVTs not so that we can conduct offensive targeting against them, but for two critical protective purposes. First, it tells us where a sophisticated threat will be most heavily defended, which are areas we should likely avoid. Second, and more importantly, it allows us to plan **lawful, non-kinetic actions** that can disrupt them. For example, if a threat's HVT is their public image of legitimacy, the SC can lawfully and ethically work with ENA Public Affairs to counter their propaganda with factual information, thereby "targeting" their HVT without ever engaging them physically. If their HVT is a specific social media account, lawfully reporting that account for terms of service violations is a valid way to disrupt their C2. This is how the SC lawfully and intelligently "fights" in the information and human domains.

5-5. The Output of Step 3: A Portfolio of Threat Models

The successful completion of Step 3 results in a critical component of our living intelligence file: a portfolio of detailed Threat Models for each significant potential hostile actor identified in our Area of Operations and Area of Interest. Each model provides a baseline understanding of a specific threat, consisting of:

1. **A Graphic Doctrinal Template** illustrating their preferred method of operation for key actions.
2. **A Descriptive Narrative** detailing their tactics, likely options (branches and sequels), and any unique peculiarities.
3. **A List of their High-Value Targets (HVTs)**, which highlights their critical vulnerabilities.

5-6. Conclusion

Step 3 of the IPOE process is an exercise in analytical rigor. It demands that we set aside our own biases and preconceived notions and evaluate potential threats based on objective, verifiable information. By systematically identifying their characteristics—composition, strength, TTPs, and support systems—we move from a vague awareness of a threat to a deep, functional understanding. The creation of detailed Threat Models codifies this understanding into a usable intelligence product. This product provides the essential doctrinal baseline of how a threat *prefers* to operate. With this critical foundation established, we are now prepared to advance to

the final, synthetic step of the IPOE process: to take these threat models and place them onto the specific environmental stage we analyzed in Step 2, and from that synthesis, to determine their most likely and most dangerous Courses of Action.

Chapter 6: Step 4 - Determine Threat Courses of Action (COAs)

6-1. Introduction

This chapter represents the culmination of our analytical efforts. It is the final and most critical step in the Intelligence Preparation of the Operational Environment process, where we move from description and evaluation to prediction. In the preceding steps, we defined our environment, analyzed its effects, and built detailed models of the potential threats within it. Now, in Step 4, we perform the essential act of synthesis. The purpose of this step is to integrate our deep understanding of the threat (from Step 3) with our comprehensive analysis of the operational environment (from Step 2) to develop a set of specific, realistic, and prioritized Threat Courses of Action (COAs).

This is the predictive core of the IPOE process. We are no longer asking “What is the terrain like?” or “How is the threat organized?” We are asking the ultimate question that drives all security planning: “What is the threat going to *do* here and now?” The outputs of this step—prioritized threat COAs, detailed Situation Templates, and a focused Event Template/Matrix—are the primary intelligence products that directly inform our own lawful friendly planning, wargaming, and information gathering efforts. A failure in this final step invalidates all the work that came before it, leaving our leaders to plan against a vague or inaccurate perception of the threat. Success, however, provides the clarity and foresight needed to develop proactive, effective, and legally sound security plans.

6-2. Identifying Threat Objectives and Desired End State

Before we can predict *what* a threat will do, we must first understand *why* they are acting. Every purposeful action is driven by an objective. Therefore, the first activity in determining threat COAs is to identify the threat’s likely objectives and their desired end state for the specific situation we are analyzing.

- **Objective:** The **objective** is the specific, tangible goal the threat seeks to achieve. It is often a physical or observable outcome. For example, the objective of a protest group might be to “shut down the city council meeting.” The objective of a criminal element might be to “steal supplies from the warehouse.”
- **Desired End State:** The **desired end state** is the broader set of conditions the threat wants to exist after the objective is achieved. It is the strategic “why” behind the tactical “what.” For the protest group, the desired end state might be “the city council’s controversial ordinance is defeated, and our group is seen as the powerful voice of the people.” For the criminal element, it might be “our group has the resources it needs to survive the next month, and law enforcement is seen as incompetent.”
- **Analysis:** To identify these, the analyst must synthesize all available intelligence. Review the threat’s core ideology and doctrine (from their Threat Model in Step 3). What are their overarching goals? Review the current situation and the specific environmental context (from Step 2). What specific opportunities or triggers exist in the environment right now? A new piece of legislation, a planned ENA event, or a disruption in the supply

chain can all create specific objectives for a threat actor. The analyst must put themselves in the threat's shoes and ask, "Given who I am, what my goals are, and the current situation, what do I want to accomplish?"

6-3. Developing the Full Set of Threat COAs

With likely objectives identified, the next activity is to brainstorm all the valid ways the threat could achieve them. A **Course of Action (COA)** is a broad potential plan. We must develop a full set of potential COAs to avoid being surprised. Each potential COA we develop must be tested against five criteria to ensure it is valid:

1. **Suitable:** Does this COA actually accomplish the threat's likely objective? If their objective is to gain media attention, a COA that involves a discreet, unseen action is not suitable.
2. **Feasible:** Does the threat have the actual capability (personnel, equipment, skills, time) to execute this COA? A plan for a complex, coordinated attack is not feasible for a small, untrained group.
3. **Acceptable:** Is the level of risk associated with this COA acceptable to the threat? A COA that would likely result in the arrest of their entire leadership might not be acceptable for a group focused on long-term influence. Conversely, for a highly radicalized group, such a risk might be perfectly acceptable. We must assess their risk tolerance based on their ideology and past behavior.
4. **Unique:** Is this COA significantly different from the others we've developed? A plan to block a road at 1 PM versus 2 PM is a minor variation, not a unique COA. A plan to block the road versus a plan to infiltrate a meeting are two unique COAs.
5. **Consistent:** Is this COA consistent with the threat's known doctrine and observed TTPs (from their Threat Model)? A group with a long history of non-violent civil disobedience is unlikely to suddenly adopt a COA involving mass casualties. While we must always be alert to a threat deviating from their patterns to achieve surprise, we must start with what is consistent with their known character.

The output of this brainstorming and vetting process is a list of all the valid, potential COAs the threat could employ to achieve their objectives in our AO.

6-4. Evaluating and Prioritizing Threat COAs

A leader cannot plan against every possibility. Our resources are finite. Therefore, we must prioritize the full set of threat COAs to focus our planning and collection efforts where they are most needed. We evaluate each valid COA to determine two key priorities:

- **Most Likely COA:** This is the COA that, based on our analysis, the threat is *most likely* to adopt. This judgment is based on several factors. It is often the COA that offers the highest probability of success with the lowest risk, is most consistent with their past behavior, and takes the best advantage of the opportunities presented by the operational environment. Our primary friendly plan should be designed to counter this Most Likely COA.
- **Most Dangerous COA:** This is the COA that, if adopted, would pose the greatest threat to the safety of the ENA community, the success of our mission, or the security of our

own SC elements. It is not necessarily the most likely. It could be a high-risk, high-impact option that the threat is unlikely to take, but one for which we must have a contingency plan. For example, the most likely COA for a protest group might be a peaceful march, but the most dangerous COA could be a “black bloc” tactic involving widespread property damage and physical assaults. We must plan for both.

The leader, based on the intelligence analyst’s assessment, makes the final determination of which COAs are considered Most Likely and Most Dangerous. These two COAs will become the primary focus of our detailed analysis and our own friendly planning and wargaming.

6-5. Developing the COA in Detail

With the priority COAs identified, we must now develop them in sufficient detail to be useful for our own planning. This involves creating two key products for each priority COA: the Situation Template and the Threat COA Statement.

a. The Situation Template (SITEMP)

- **Purpose:** A **Situation Template** is a graphic depiction of a specific threat COA as it would unfold in our Area of Operations at a critical time and place. It is the result of taking the threat’s “doctrinal template” (from Step 3) and overlaying it onto our specific environmental analysis (the MCOO from Step 2), adjusting it based on how the real-world environment would force the threat to act.

- **Creation:** To create a SITEMP, the analyst:

Starts with the Doctrinal Template: Takes the graphic from the Threat Model showing how the threat *prefers* to operate.
Integrates Environmental Effects: Places this template onto the MCOO of the relevant area in the AO. The analyst must then think like the threat commander. How does the terrain force me to change my ideal plan? The river and the single bridge (obstacles) will canalize my movement. The high ground on Patriot’s Ridge (key terrain) is the best place for my observation posts. The dense forest (concealment) is the best infiltration route. The SITEMP shows the threat’s plan as modified by the realities of the ground.
Depicts Key Actions: The SITEMP should graphically depict the threat’s dispositions, their scheme of maneuver (with arrows), and the location of their key assets at the most critical moment of their operation (e.g., the moment a protest line is established, or the moment an ambush is initiated). It can also include time-phase lines to show their expected rate of movement.

- **Value:** The SITEMP is a powerful predictive tool. It transforms an abstract threat model into a concrete picture of a potential reality. It is the primary intelligence product used during our own friendly wargaming to test our plans against a specific, visualized threat action.

b. The Threat COA Statement

- **Purpose:** The **Threat COA Statement** is a concise narrative that accompanies and describes the graphic SITEMP. It answers the six key questions for the specific COA: Who, What, When, Where, How, and Why.

- **Content:** The narrative must include:
  - **Objective (Why):** A clear statement of what the threat is trying to accomplish with this COA.
  - **Disposition and Task Organization (Who/Where):** A description of the forces the threat will use and where they will be positioned, as depicted on the SITEMP.
  - **Scheme of Maneuver (How):** A description of how the threat will execute their plan from start to finish.
  - **Timeline (When):** The earliest time the threat could initiate this COA.
  - **HVTs:** A list of the specific HVTs for *this* COA.
- **Value:** The COA Statement provides the essential context and detail for the SITEMP graphic. Together, the SITEMP and the COA Statement provide a complete and understandable picture of a single priority threat COA.

6-6. Developing the Event Template and Event Matrix

Once we have developed detailed SITEMPs for our priority threat COAs (at a minimum, the Most Likely and Most Dangerous), our final task is to create the tools that will help us determine which COA the threat has actually chosen. This is the purpose of the Event Template and Event Matrix.

a. The Event Template

- **Purpose:** The **Event Template** is a single graphic overlay that consolidates the key indicators from all of the different threat SITEMPs. Its purpose is to identify the **Named Areas of Interest (NAIs)**—the specific locations in our AO where we need to collect information to confirm or deny which COA the threat has adopted.
- **Creation:** To create an Event Template, the analyst:

Compares the SITEMPs: The analyst lays the SITEMPs for the Most Likely COA and the Most Dangerous COA (and any other priority COAs) on top of each other.
Identifies Differences: The analyst looks for activities that are *unique* to a specific COA. For example, if the Most Likely COA involves a protest at the courthouse, but the Most Dangerous COA involves staging in the industrial park to block the interstate, then the courthouse and the industrial park become key points of difference. Activity that is common to both COAs (like using a specific social media page for general messaging) is less useful for differentiation.
Designates NAIs: The locations where these unique, discriminating activities would occur are designated as Named Areas of Interest. An NAI is a point or area where activity—or a lack of activity—will provide a significant clue as to the threat's intentions. The Event Template is simply a map of our AO with all the NAIs for our priority COAs plotted on it.

- **Value:** The Event Template is the primary tool for focusing our limited intelligence collection assets. It tells our observation posts, our patrols, and our OSINT analysts exactly where to look and what to look for.

b. The Event Matrix

- **Purpose:** The **Event Matrix** is a table that supports the graphic Event Template. It provides the detailed "so what?" for each NAI, linking the location to specific indicators and the COA they confirm or deny.

- **Content:** The Event Matrix has several key columns:
  - **NAI:** The number or name of the Named Area of Interest from the Event Template.
  - **Indicator:** A description of the specific, observable activity we are looking for in that NAI. (e.g., “Presence of more than 10 members of Group X,” or “Delivery of construction materials suitable for building barriers.”)
  - **Time:** The likely time (or time window) that we would expect to see this indicator, based on our analysis of the threat’s timeline.
  - **COA Indicated:** Which specific threat COA this indicator would confirm or deny.

NAI	Indicator	Time (H-Hour)	COA Indicated
NAI 1 (Courthouse)	Presence of >10 Group X members with signs and banners.	H-2 to H-1	COA 1 (Most Likely): Protest
NAI 2 (Industrial Park)	Presence of vehicles carrying tires, lumber, or barrels.	H-4 to H-2	COA 2 (Most Dangerous): Blockade
NAI 3 (Online Forum)	Posts calling for “direct action” and protective gear.	H-12 to H-4	COA 2 (Most Dangerous): Blockade

- **Value:** The Event Matrix is a powerful tool for our collection elements and analysts. It provides a simple, at-a-glance guide for interpreting events as they unfold. When an OP reports a specific indicator from the matrix, the leader can immediately understand its potential significance and which threat COA is becoming more probable, allowing for timely and informed decisions.

6-7. The Output of Step 4: Predictive Intelligence

The successful completion of Step 4 of the IPOE process provides the SC leader with a powerful set of predictive intelligence products that are ready to be integrated into our own friendly planning process:

1. **A Prioritized List of Threat COAs,** identifying at a minimum the threat’s Most Likely and Most Dangerous options.
2. **Detailed Situation Templates (SITEMPs) and Threat COA Statements** for each priority COA.
3. **A Consolidated Event Template and Event Matrix** that will drive our information gathering plan.

6-8. Conclusion

Step 4 is the crucible of the IPOE process. It is where we forge raw data and separate analyses into the sharp, actionable tool of predictive intelligence. By identifying threat objectives, developing a full set of valid COAs, and then rigorously evaluating and prioritizing them, we focus our efforts on the most significant possibilities. The detailed development of Situation Templates translates these possibilities into concrete, visual realities that we can plan against and wargame. Finally, the creation of the Event Template and Matrix gives us a systematic, lawful plan for monitoring the environment to discover the threat’s true intentions. With these products in hand, the IPOE process is complete. We have moved from a state of simple awareness to one of deep, predictive understanding. We are now fully prepared to use this intelligence to drive our own planning and to fulfill our mission of lawfully safeguarding the Euramerican community

from a position of profound knowledge.

Chapter 7: IPOE and the SC Planning Process

7-1. Introduction: From Understanding to Action

The preceding chapters have meticulously detailed the four-step process of Intelligence Preparation of the Operational Environment. We have defined our environment, described its effects, evaluated the threats within it, and determined their likely Courses of Action. This rigorous analytical work, however, is not an end in itself. Its entire purpose is to serve as the foundation for our own planning and action. Intelligence that does not inform a decision is merely academic. This chapter bridges the critical gap between understanding and action, explicitly linking the products of the IPOE process to the Security Corps' planning methodology: the adapted Troop Leading Procedures (TLP), as detailed in SCDP 5-0, *Planning*.

The TLP is the logical, step-by-step process our leaders use to translate an assigned mission into a feasible, acceptable, suitable, and, above all, lawful plan. IPOE is the engine that drives this process. It provides the essential situational awareness and predictive intelligence that fuels each step of the TLP, from the initial mission analysis to the final supervision of rehearsals. This chapter will demonstrate, step by step, how the outputs of our IPOE—the MCOO, the Threat Models, the Situation Templates, and the Event Template/Matrix—are not just reference documents but are active, indispensable tools used to craft superior, intelligence-driven plans. Understanding this direct and practical link is essential for every SC leader seeking to transform their analytical efforts into effective, lawful operations.

7-2. Supporting Mission Analysis (TLP Step 1 & 3)

Mission analysis is the heart of the TLP. It is where the leader and their element deconstruct an assigned mission to fully understand the task, the environment, and the challenges they face. The IPOE process provides the bulk of the information and analysis required for a thorough mission analysis, specifically through the framework of METT-TC (Mission, Enemy/Threat, Terrain and Weather, Troops and Support Available, Time Available, and Civil Considerations).

- **Enemy/Threat:** The question "Who is the threat and what are their capabilities?" is answered directly by the outputs of **IPOE Step 3: Evaluate the Threat**. The detailed **Threat Models**—including the threat's composition, strength, TTPs, and High-Value Targets (HVTs)—provide a comprehensive picture of the adversary. This allows the leader to move beyond vague notions of a threat and begin to analyze a specific, well-understood entity.
- **Terrain and Weather:** The analysis of the physical environment is provided directly by **IPOE Step 2**. The **Modified Combined Obstacle Overlay (MCOO)** graphically depicts the ground, highlighting Avenues of Approach, Key Terrain, and Obstacles. The **Terrain and Weather Effects Matrices** provide a concise written summary of how the physical environment will impact both our own and the threat's operations. This allows the leader to conduct a rapid and effective OAKOC/KOCOA analysis, which is fundamental to understanding the "battlefield."
- **Civil Considerations:** The complex human domain is analyzed in **IPOE Step 2**. The

Civil Considerations Assessment, derived from the PMESII-PT analysis, provides the leader with the necessary understanding of the social, political, and economic landscape. It identifies key leaders, social fault lines, influential groups, and, critically, the **Legal Framework** that will govern the operation. This is essential for planning lawful actions that maintain community legitimacy.

By leveraging these pre-developed IPOE products, an SC leader can conduct a rapid yet thorough mission analysis. The foundational work has already been done. Instead of starting from scratch, the leader can immediately begin to synthesize this information, identify the essential tasks, and formulate a clear understanding of the operational problem they have been tasked to solve.

7-3. Supporting Friendly Course of Action (COA) Development (TLP Step 3)

Once mission analysis is complete, the leader develops one or more friendly Courses of Action (COAs) to accomplish the mission. This is a creative process, but it must be grounded in reality. The IPOE products provide this essential grounding, ensuring that our friendly COAs are not just clever, but also effective, realistic, and legally sound.

- **Informing the Scheme of Maneuver:** How we will move and position our elements is directly informed by the **MCOO** and **Terrain Effects Matrix**. A leader will plan their routes along viable mobility corridors, seek to control or monitor the identified **Key Terrain**, and use **Obstacles** to their advantage while avoiding those that would hinder their own movement. Our scheme of maneuver is a direct response to the opportunities and constraints of the physical terrain as analyzed in IPOE Step 2.
- **Countering the Threat:** Our friendly COA must be designed to counter the threat. The detailed **Threat Models** from IPOE Step 3 and the prioritized **Threat COAs** from Step 4 are the primary tools for this. We design our plan to:
    - **Avoid Threat Strengths:** If the threat's TTPs show they are highly proficient in conducting ambushes from concealed positions, our friendly COA will prioritize routes that offer good observation and avoid canalizing terrain.
    - **Exploit Threat Weaknesses:** If the threat is known to have poor communications discipline, our plan might include an information gathering effort focused on exploiting that vulnerability (lawfully).
    - **Deny Threat Objectives:** If we have identified the threat's likely objective, our COA can be designed to proactively deny them that objective, for example, by establishing a lawful security presence at their intended target location before they arrive.
    - **Target Threat HVTs (Lawfully):** By knowing the threat's High-Value Targets, we can develop lawful, non-kinetic actions to disrupt them. If their HVT is their C2 network, our plan might include efforts to lawfully report their communications platforms for terms of service violations.
- **Ensuring Legal Compliance:** The **Legal Framework** summary, a key product of the human domain analysis in IPOE Step 2, is a non-negotiable input to COA development. Every action considered for our friendly COA—from the placement of an OP to the procedures for access control—must be checked against this framework. A COA that

includes an illegal action is not a valid COA.

The IPOE process ensures that our friendly COAs are developed in direct response to the realities of the environment and the specific nature of the threat, rather than being based on abstract templates or wishful thinking.

7-4. Supporting Wargaming (TLP Step 4)

Wargaming is the critical step where we test our friendly COA against the threat's likely actions. It is a mental simulation of the operation, an action-reaction-counteraction drill designed to identify flaws in our plan and develop contingencies. This process is impossible without the predictive intelligence products from IPOE Step 4.

- **The "Red Team" Script:** The **Situation Templates (SITEMPs)** for the threat's **Most Likely** and **Most Dangerous** COAs serve as the script for the "red team" during the wargame. The leader or analyst playing the role of the threat does not have to guess what the threat will do; they simply execute the actions laid out in the SITEMP.
- **The Wargaming Process:** The leader walks through their friendly plan, step by step. At each critical point, the person playing the threat responds based on the SITEMP: "As your security element approaches the Miller Bridge, my observation post on Patriot's Ridge, as depicted on the SITEMP for my Most Likely COA, observes your movement and reports it to my leader." The friendly leader must then decide on a counteraction.

This process allows us to:

- **Identify Friction Points:** We can see where our plan is weak or where it is likely to come into conflict with the threat's plan.
- **Test Assumptions:** We can validate or invalidate the assumptions we made during planning.
- **Develop Contingencies:** When a friction point is identified, we can develop a specific contingency plan (a branch) to address it.
- **Synchronize Actions:** We can see how the actions of different friendly elements need to be synchronized to be effective.

Without the detailed SITEMPs from the IPOE, wargaming would be an exercise in pure speculation. With them, it becomes a powerful and disciplined analytical tool for refining our plan and preparing our element for the realities of the mission.

7-5. Developing the Information Gathering Plan

A core output of the planning process is a detailed, lawful plan to collect the information we still need. The primary tool for developing this plan is the **Event Template** and **Event Matrix** from IPOE Step 4. These products are designed for exactly this purpose.

- **Focusing the Collection Effort:** The leader's **Information Needs** are the questions that must be answered. The Event Template, with its identified **Named Areas of Interest (NAIs)**, tells us *where* to look for the answers. The Event Matrix tells us *what specific indicators* to look for in each NAI and *what those indicators mean*.

- **The Planning Process:**

Review the Information Needs: The leader confirms their priority intelligence questions.
Consult the Event Template/Matrix: The analyst identifies which NAIs and indicators from the matrix are directly relevant to the leader's Information Needs.
Task Collection Assets: The leader assigns specific SC assets to lawfully collect on those NAIs. This involves creating a simple **Information Gathering Plan**. For example:

  - "**Team Alpha (Collection Asset)** will establish a lawful **Observation Post (Collection Task)** at **NAI 1 (Location)** to determine if **more than 10 members of Group X are present (Indicator)**. Report immediately if observed."
  - "**Designated OSINT Analyst (Collection Asset)** will lawfully monitor the **online forum at NAI 3 (Location)** to determine if there are **posts calling for 'direct action' (Indicator)**."

- **Legal Compliance:** The information gathering plan must be rigorously vetted for legal compliance. Every collection task assigned must specify a lawful method. This plan transforms our intelligence collection from a passive, reactive process into a proactive, targeted, and lawful hunt for the specific information needed to confirm or deny the threat's intentions and provide the leader with decision-making superiority.

7-6. Supporting Assessment

Assessment is the continuous process of evaluating the effectiveness of our operations. It is the "Assess" phase of the SC Action Cycle. The IPOE provides the essential baseline against which all assessment is made.

- **Establishing the Baseline:** The entire IPOE product—the MCOO, the Civil Considerations Assessment, the Threat Models—represents our best understanding of the operational environment *before* our operation begins. This is the baseline state.
- **Measuring Change:** During and after an operation, we collect new information. Assessment is the process of comparing this new information to our IPOE baseline.
  - Did our actions have the intended effect? The IPOE identified a threat HVT as their public legitimacy. Our operation included a lawful information campaign to counter their propaganda. Assessment involves measuring the change in public sentiment (through lawful monitoring of the information environment) to see if our campaign was effective.
  - Is the threat reacting as we predicted? The IPOE produced SITEMPs for the threat's Most Likely and Most Dangerous COAs. Assessment involves comparing the threat's actual actions to these SITEMPs. If they are following their Most Likely COA, our primary plan is likely sound. If they are shifting toward their Most Dangerous COA, we may need to execute a contingency plan.
  - Has the environment changed? The IPOE established a baseline of community stability. Assessment involves monitoring that stability. Are our actions increasing or decreasing tensions? This feedback is critical for maintaining legitimacy and ensuring we are not inadvertently making the situation worse.

Without the detailed baseline provided by a thorough IPOE, assessment becomes a subjective and unreliable guess. With it, assessment becomes a disciplined process of measuring change

against a known starting point, allowing us to learn, adapt, and improve our effectiveness over time.

7-7. Conclusion

Intelligence Preparation of the Operational Environment is not a separate, academic staff exercise. It is the living, breathing heart of the Security Corps planning process. As this chapter has demonstrated, the products of each step of the IPOE are not artifacts to be filed away; they are the essential tools and inputs for each corresponding step of the TLP. IPOE provides the environmental context for mission analysis, the threat picture that shapes our friendly COA development, the predictive SITEMPs that make our wargaming realistic, and the focused Event Template that drives our lawful information gathering. Finally, it establishes the critical baseline against which we assess our own effectiveness. By mastering the direct integration of IPOE into our planning process, SC leaders ensure that our actions are not based on hope or assumption, but on a deep, predictive, and multi-domain understanding of the world in which we operate. This is the hallmark of a professional security element and the very essence of the proactive advantage.

Chapter 8: The Living File - Continuous Assessment

8-1. Introduction

You have now completed the demanding intellectual journey of the four-step Intelligence Preparation of the Operational Environment process. You have defined your environment, described its effects, evaluated the threats within it, and determined their likely Courses of Action. The result of this effort is a comprehensive intelligence product—a binder, a digital folder—that represents a high-resolution snapshot of your Area of Operations at a specific moment in time. This is a monumental achievement and the foundation of all sound security planning. However, the single most critical mistake an analyst or leader can make at this point is to place that product on a shelf and consider the job "finished."

The operational environment is not a static photograph; it is a live, streaming video. It is a complex, adaptive system in a constant state of flux. Political alliances shift, economic conditions evolve, new social tensions emerge, infrastructure is built or decays, and threats adapt their tactics. An IPOE product that is not actively maintained loses its value with each passing day, becoming a historical document rather than a tool for decision-making. This final chapter is dedicated to the most important discipline in the intelligence lifecycle: transforming your static product into a living intelligence file. This is accomplished through the continuous process of **Area Assessment**, which ensures that your hard-won understanding remains sharp, relevant, and predictive, solidifying the proactive advantage for the long term.

8-2. The Study is Never "Finished": From Static Product to Living File

Think of your newly completed IPOE as the foundational architectural blueprint for a building. It is the indispensable starting point, providing the essential structure and layout. But a building is not a static object; it is an ecosystem. Its occupants change, its systems require maintenance, and it is constantly battered by the elements. A good building manager doesn't just rely on the original blueprints; they conduct regular inspections, monitor systems for signs of wear, and stay aware of how the building's use is changing over time.

Your relationship with your IPOE product must be that of a steward. The initial four-step process was the hard work of creating the baseline understanding. The work from this point forward is the discipline of continuous assessment—the process of keeping that baseline current. A static IPOE, left untouched for a year, develops a dangerous "relevancy gap"—a growing delta between your perception of reality and reality as it actually exists. Decisions made from within this gap are, by definition, based on flawed or outdated intelligence. Such decisions are not just ineffective; they are a direct threat to the safety of our members and the legitimacy of our operations.

A living intelligence file, however, is a dynamic and powerful tool. It is a repository of your current, best understanding of the environment, designed to absorb new data, discard the obsolete, and highlight emerging trends. This does not mean you must rewrite the entire study every week. It means you must have a simple, sustainable process for observing your environment, identifying significant changes, and updating the relevant sections of your study. This is the Assessment Cycle, the practical application of the "Assess" phase of the SC Action

Cycle.

8-3. The Assessment Cycle: A Habit of Mind

The Assessment Cycle is a simplified, continuous loop that allows us to efficiently maintain our IPOE file. It is a mental checklist that should become a habit of mind for every SC leader and intelligence analyst, ensuring our knowledge never goes stale. It consists of three simple, repeating steps: Validate Old Information, Collect New Information, and Identify New Gaps.

Step 1: Validate Old Information

This is the process of intellectual housekeeping. Before seeking out new information, you must first ask, “Is what I know still true?” This involves a periodic review of the key judgments and foundational facts in your IPOE.

- **Example (Political):** Your IPOE lists the current members of the city council. The validation task is a quick visit to the official city government website to confirm that no resignations, appointments, or special elections have occurred. If a member has changed, that section of your file must be updated.
- **Example (Infrastructure):** Your IPOE identifies the Miller Bridge as a key chokepoint. The validation task could be a quick search on the State Department of Transportation website. Is the bridge still open? Has its weight limit been changed? Is there any new, long-term construction scheduled that would affect its capacity?
- **Example (Threat):** Your IPOE identifies a specific social media page as the primary C2 platform for a local activist group. The validation task is to lawfully and passively check if that page is still active or if they have migrated to a new platform.

Validation is the process of confirming your baseline. If your key facts are no longer correct, the entire analytical structure built upon them is at risk.

Step 2: Collect New Information

This is the forward-looking part of the cycle, focused on the question, “What has changed?” This involves an active, but not necessarily intensive, scanning of the information environment for significant new developments that could alter your previous assessments.

- **Example:** While lawfully monitoring the local news (part of your routine), you see an article announcing that the county’s largest employer is planning to lay off 30% of its workforce (**Economic**). This is a significant piece of new information. It will directly impact the **Social** domain (increased unemployment, potential for unrest), the **Political** domain (pressure on elected officials to respond), and potentially the **Military (LE)** domain (potential for increased crime). This single piece of new data triggers a need to update multiple sections of your IPOE and reassess the stability of the entire AO.

Step 3: Identify New Gaps

The process of validating old information and collecting new information will inevitably reveal things you don’t know. Identifying an intelligence gap is not a failure; it is a sign of a healthy and functioning intelligence process. It is an opportunity to improve your understanding.

- **Example:** In the layoff scenario above, you have collected the “what” (a major layoff is coming). This immediately creates new information gaps. “What is the specific timeline

for the layoffs?" "What are the local government's plans, if any, to provide support for the displaced workers?" "Are any of the identified ideological groups using this event to recruit or spread propaganda?" Each of these questions becomes a new, specific **Information Need** that can be tasked out in your next focused collection effort.

This three-step cycle—**Validate, Collect New, Identify Gaps**—is the engine of your living intelligence file. It creates a continuous feedback loop that constantly refines and improves your understanding of your AO, ensuring your proactive advantage is never lost.

8-4. Indicators and Warnings (I&W): Your Tripwire System

To make the Assessment Cycle efficient, you cannot possibly track every piece of information all the time. You need a system to help you focus on what's important. This system is called **Indicators and Warnings (I&W)**.

- An **Indicator** is a discernible piece of information or an observable event that suggests a potential change in the state of the environment.
- A **Warning** is an indicator or a group of indicators that suggests a negative or threatening change is imminent or already underway.

Think of indicators as your environment's "check engine light." They don't always mean catastrophe is imminent, but they signal that something has changed and requires your focused attention. Your primary source for developing a tailored I&W list is the **Event Matrix** you created in IPOE Step 4. The indicators you identified to differentiate between threat COAs are the perfect starting point. The analyst should pre-identify a list of simple, easy-to-observe indicators across the PMESII-PT domains. When you observe one of these indicators, it acts as a mental tripwire, triggering you to investigate further and ask, "So what?"

Sample Indicators for an SC Element:

- **(P) Political:** A sudden, unscheduled emergency meeting of the city council. The introduction of a controversial new ordinance that is known to be a trigger for local activist groups.
- **(M) Military / LE:** A noticeable increase in law enforcement patrols in a specific neighborhood. A public announcement by the Sheriff's Office about a credible threat to the community.
- **(E) Economic:** A sudden spike in local fuel prices that is disconnected from national trends. The unexpected closure of a major retail store. Widespread shortages of a basic commodity like baby formula or ammunition.
- **(S) Social:** A sudden spike in graffiti or online rhetoric associated with an identified extremist group. The planning of a protest and a counter-protest for the same time and location (this is a **Warning** of potential conflict).
- **(I) Information:** The emergence of a powerful new disinformation campaign on local social media. A local media outlet reporting on a specific threat to the ENA or its members.
- **(I) Infrastructure:** The appearance of survey markers and utility flags along a critical evacuation route (Indicator of impending construction and potential disruption). A widespread, unexplained power or communications outage.
- **(P) Physical Environment:** An official declaration of a burn ban or drought warning. A severe weather watch or warning issued for your AO.

- **(T) Time:** The approaching anniversary of a past contentious event or riot.

By maintaining a mental or written list of indicators relevant to your AO, you train your brain what to look for. You are no longer a passive consumer of information; you are an active analyst scanning your environment for signals of change. When an indicator is tripped, you can then focus your collection and analysis efforts to understand its implications, keeping your IPOE file sharp and predictive.

8-5. A Sustainable Routine for Volunteers

A process that is not scheduled is a process that will not happen. For a volunteer force, it is absolutely essential that the maintenance of the IPOE file be integrated into a regular routine that is manageable and sustainable. A process that requires hours of work every day is a process that will be abandoned. The key is to adopt a tiered approach to your reviews.

The Weekly Scan (15-30 Minutes)

This is your quick, routine check-in to maintain basic situational awareness. It should be a fixed part of your weekly schedule, for example, every Sunday evening.

- **Actions:**
  - Skim the headlines of the primary local newspaper's website for the past week.
  - Briefly review the official websites and public social media feeds of your county emergency management agency and sheriff's office for any new alerts or press releases.
  - Lawfully and passively scan any key local online forums or social media groups you have identified as part of your informal information network analysis.
- **Goal:** The purpose of this scan is simply to spot any major new events or tripped indicators that require more immediate attention or a quick update to your file. It is the "pulse check" of your AO.

The Quarterly Deep Dive (1-2 Hours)

Every three months, schedule a longer session to do a more focused update. To make this manageable, break up the PMESII-PT framework over the course of the year. This prevents the daunting task of reviewing the entire binder at once.

- **Example Schedule:**
  - **Q1 (January-March): Focus on the Physical and Infrastructure Domains.** Review your MCOO. Are there any new major construction projects affecting your AAs? Have you physically reconnoitered your alternate routes recently? Is your data on key infrastructure nodes still accurate?
  - **Q2 (April-June): Focus on the Political and Economic Domains.** Was there a recent local election? Has the list of key elected officials changed? Is your list of major employers still accurate? Have there been any significant shifts in the local economy?
  - **Q3 (July-September): Focus on the Social and Information Domains.** Have any new activist or threat groups emerged? Have the tactics of existing groups changed? Has the local media landscape shifted? Re-validate your understanding of the key social fault lines.
  - **Q4 (October-December): Focus on Threat Models and Friendly Plans.** Review

your Threat Models from Step 3. Is your assessment of their TTPs and capabilities still valid? Most importantly, review your own friendly plans (security, contingency, logistics) that were derived from the IPOE. Are they still relevant and feasible based on the updates you've made throughout the year?

- **Goal:** This breaks the review process into manageable quarterly chunks, ensuring every section of your IPOE gets a detailed look at least once a year.

The Annual Full Review (Half-Day)

Once a year, set aside a few hours to conduct a top-to-bottom review and refresh of your entire IPOE product.

- **Actions:**
  - Go through your entire binder or digital file page by page, validating all key facts and assessments.
  - Update all of your key contact lists and legal framework summaries.
  - Print fresh copies of your most critical maps and overlays if you maintain a physical binder.
  - **Most importantly, rewrite your Executive Summary.** Your top-line judgments and overall assessment of the AO will almost certainly have evolved over a year. Rewriting this single page is the best way to synthesize your current, holistic understanding and to codify the results of your year-long assessment cycle.
- **Goal:** This ensures the integrity and relevance of the entire product and marks a definitive end to one year's assessment cycle and the beginning of the next.

8-6. Conclusion

The discipline of continuous assessment is what transforms the IPOE from a one-time project into a career of informed vigilance. It is the commitment that ensures the knowledge you have worked so hard to build remains your most powerful and reliable tool for mastering your environment. By embracing the concept of the living file, practicing the simple three-step Assessment Cycle, using an I&W list to focus your attention, and adopting a sustainable routine, you institutionalize the proactive advantage. This disciplined habit is the final and most crucial element of the IPOE framework. It ensures that no matter how much the world may change, your understanding will change with it, keeping you and the Euramerican community you protect one step ahead.

Conclusion: The Proactive Advantage

You have reached the end of this guide, but you stand at the beginning of a new way of seeing the world. The journey you have undertaken through these pages was designed to be transformative. It was intended to guide you from the perspective of a passive resident, subject to the whims of an unpredictable environment, to that of an informed analyst, capable of understanding, anticipating, and lawfully acting within that same environment. We began with a simple premise—that knowledge is power—and we have systematically deconstructed that premise, forging it from an abstract slogan into a tangible, actionable methodology.

The process of Intelligence Preparation of the Operational Environment, as you have learned, is far more than a mere collection of facts to be compiled into a static report. It is a rigorous intellectual discipline, a living intelligence file, and the indispensable foundation for all effective, lawful security planning. It is the Security Corps' formal methodology for mastering the first and most critical phases of the OOD Loop—**Observe and Orient**. By dedicating ourselves to this process, we seize control of our own perception, refusing to allow it to be shaped by hostile narratives, incomplete information, or unfounded fear. We choose instead to build our own clear, coherent, and reality-based orientation to the world. It is from this position of superior orientation that we are empowered to make better decisions, faster, and more lawfully than any potential adversary, which is the very definition of a decisive advantage.

We deconstructed the staggering complexity of the world around us using the comprehensive PMESII-PT framework, ensuring no critical domain was left unexamined. We explored the solid, tangible realities of the Physical Environment, learning to read the terrain not as scenery, but as a strategic landscape of corridors, chokepoints, and key terrain. We mapped the man-made skeleton of Infrastructure, identifying the critical nodes and fragile systems upon which modern life depends.

We then delved into the infinitely more complex and dynamic Human Domain. We analyzed the social fault lines, the cultural currents, and the ideological actors that animate the communities in which we operate. We learned to objectively and dispassionately catalog potential threats from across the ideological spectrum, focusing on capability and intent rather than political labels. We mapped the formal and informal structures of the Political and Economic domains, building an understanding of who is in charge, who wields force, what truly makes the community run, and, most critically, the specific legal framework that forms the non-negotiable boundaries for all our actions.

We did not stop at mere description. We learned that data without analysis is useless. Through the four-step IPOE process, you learned how to transform information into intelligence. You learned to build Threat Models to understand your adversaries as they see themselves. You learned to synthesize your knowledge of the threat and the environment to develop predictive Situation Templates. And you learned to create Event Templates and Matrices, turning your predictive analysis into a focused, lawful plan for information gathering that can confirm or deny a threat's intentions. Finally, we translated that hard-won intelligence into actionable planning considerations, linking the IPOE directly to the SC's adapted Troop Leading Procedures and demonstrating how superior knowledge informs every aspect of our operations.

This process has given you a profound strategic advantage. While others may see the world

through a fog of media-driven narratives and vague, free-floating anxieties, you now possess the tools to see it with clarity. You can see the systems, the networks, and the vulnerabilities. You understand the players, their motivations, and their likely courses of action. When a crisis unfolds—whether it's a natural disaster, a supply chain disruption, or an outbreak of civil unrest—you will not be a passive victim of circumstance. You will be an informed actor, capable of anticipating events rather than merely reacting to them. This is the **proactive advantage**, and it is the ultimate form of preparedness. It is the difference between being a leaf tossed about in the stream and being the person standing on the bank, observing the current, understanding its power, and choosing where and when to lawfully cross.

More important than the binder you have created, however, is the mindset you have cultivated. The true goal of this doctrine was not simply to teach you how to build a product, but to help you internalize a new way of thinking. The greatest benefit of the IPOE process is that it fundamentally rewires your brain. You can no longer drive through your town without subconsciously noting the avenues of approach, the location of the electrical substation, or the security posture of a key facility. You cannot watch the local news without filtering the information through your understanding of the area's political fault lines and key players.

You have learned to practice the art of constant, structured observation and analysis. This is a mindset of disciplined curiosity, a permanent habit of scanning your environment for the indicators of change you have learned to identify. It is the quiet, confident awareness that comes from knowing the baseline of "normal" in your Area of Operations so well that you can immediately spot an anomaly and begin to lawfully and logically assess its implications. This mindset is your most portable and powerful tool. It costs nothing, weighs nothing, and can never be taken from you. It is the personal software that runs in the background, constantly updating your orientation to the world and keeping your intelligence file relevant and sharp.

In completing this work, you have embarked on the path to becoming the "local expert." This is not a title of arrogance, but a statement of quiet, professional competence. It means that for your chosen Area of Operations—your home, your family, your community—you are now the single most reliable source of integrated, multi-domain, lawfully-derived intelligence. You are the person who has done the homework. You are the one who has read the boring municipal planning documents, traced the supply chains, and mapped the chokepoints. You are the one who understands not just what is happening, but *why* it is happening, and what is likely to happen next.

This expertise is the bedrock of true self-reliance and effective community protection. It replaces fear of the unknown with a calm confidence grounded in facts and rigorous analysis. It empowers you to lead, to make sound, lawful judgments for yourself and your element, and to be a resource of immense value to the Security Corps and the ENA should the need arise. In a world of increasing complexity and uncertainty, the ability to generate your own clarity is the ultimate skill.

The journey you began with Chapter 1 does not end here. Your IPOE is a living document, and the environment it describes is in constant flux. The discipline of the assessment cycle—of validating, collecting, and identifying new gaps—is now yours to practice. The proactive advantage is not a one-time achievement; it is a state that must be maintained through continuous vigilance and intellectual rigor.

Look at the product you have created. It is the physical proof of your dedication. It is a tool, a reference, a plan. But more than that, it is a symbol of a promise you have made to yourself and to the Euramerican community: a promise to see the world clearly, to think critically, to prepare intelligently, and to no longer be a passive observer of the forces that shape your life. You have chosen to be proactive. You have chosen to be prepared. You have chosen knowledge over fear. And that is the most powerful choice of all.

Appendix A: Glossary of Key Terms

This glossary defines key terms and acronyms as they are used within the specific context of the Euramerican National Assembly (ENA) Security Corps (SC) doctrine, particularly SCDP 2-01.3. A shared, precise vocabulary is essential for clear communication, shared understanding, and the effective, lawful execution of all SC intelligence and planning functions.

Adaptive Command The Security Corps' command and control philosophy that empowers subordinate leaders to exercise **Disciplined Initiative** within the **Leader's Intent** and strict legal and ethical boundaries. Intelligence Preparation of the Operational Environment provides the essential situational understanding that enables this philosophy to function effectively.

Area Assessment The continuous process of monitoring the operational environment to keep the IPOE product (the living file) current. It involves the cycle of validating old information, collecting new information, and identifying new intelligence gaps.

Area of Interest (AI) The broader geographic region that contains threats, influences, or other factors that can affect operations within the Area of Operations (AO). The AI provides strategic context, and is monitored with less detail than the AO.

Area of Operations (AO) The specific, defined geographic area where the SC element is assigned to conduct its mission. It is the primary focus of the IPOE effort, requiring intimate, granular knowledge.

Course of Action (COA) (Threat) A broad potential plan a threat actor could take to accomplish their objectives. For a COA to be considered valid during analysis, it must be Suitable, Feasible, Acceptable, Unique, and Consistent with the threat's known patterns.

Cover Protection from the effects of fires (e.g., bullets, shrapnel). It is provided by features that will physically stop projectiles, such as thick concrete walls or large earth berms. Not to be confused with **Concealment**.

Concealment Protection from observation, but not from the effects of fires. It is provided by features that can hide a person or object from view, such as vegetation, smoke, or camouflage. Not to be confused with **Cover**.

Disciplined Initiative Action taken by subordinates, consistent with the leader's intent and doctrine, to proactively address opportunities or threats in the absence of specific orders or when the existing plan no longer applies, always within legal and ethical boundaries.

Doctrinal Template (Threat) A graphic product of the Threat Model (IPOE Step 3) that illustrates how a threat *prefers* to organize and deploy its capabilities to conduct a specific type of operation, unconstrained by the environment. It represents their "textbook" solution.

Euramerican National Assembly (ENA) The representative political body of the Euramerican national community, which provides the strategic direction, authority, and resources for the Security Corps.

Event Matrix A table that supports the **Event Template**. It links specific **Named Areas of Interest (NAIs)** to observable **Indicators**, timelines, and the specific threat **Course of Action**

(COA) they would confirm or deny.

Event Template A single graphic overlay, created in IPOE Step 4, that consolidates key indicators from different threat **Situation Templates**. Its purpose is to identify **Named Areas of Interest (NAIs)** where information must be collected to determine which COA the threat has adopted. It is the primary tool for developing the Information Gathering Plan.

High-Value Target (HVT) An asset that the *threat commander* requires for the successful completion of their mission. For the SC, HVTs are identified not for offensive targeting, but to understand threat vulnerabilities and to plan for lawful, non-kinetic disruption.

Human Domain A term encompassing the social, political, and economic aspects of the operational environment, as analyzed through the PMESII-PT framework. It deals with the people, their culture, their systems of governance, and their means of subsistence.

Indicator A discernible piece of information or an observable event, often tied to a specific time and place, that suggests a potential change in the situation or points to a threat's intentions or capabilities.

Indicators and Warnings (I&W) A system of pre-identified **Indicators** that serve as a "tripwire" to focus an analyst's attention on significant changes in the operational environment, prompting further investigation and assessment.

Information Gathering Plan The specific, lawful plan for collection that is an output of the planning process. It tasks specific SC elements to collect on specific **Named Areas of Interest (NAIs)** and **Indicators** derived from the Event Template/Matrix in order to answer a leader's Information Needs.

Information Need A specific question about the operational environment that a leader needs answered to make a timely and informed decision or to complete a plan. Information Needs drive the IPOE process.

Intelligence Preparation of the Operational Environment (IPOE) The systematic, continuous process of analyzing the threat and the environmental variables of Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-PT) within a specific Area of Operations to determine their effect on the Security Corps' ability to safeguard the Euramerican national community, its rights, and its future.

Key Terrain Any locality or area whose seizure, retention, or control affords a *marked advantage* to either side. It is terrain whose control is decisive to the outcome of operations in that area.

Leader's Intent A clear, concise statement of the purpose of an operation, the key tasks required to be accomplished, and the desired lawful end state. It is the cornerstone of **Adaptive Command**.

Legal Framework The collection of applicable federal, state, and local laws, statutes, and ordinances, as well as ENA policies and ROE, that govern SC operations within a specific jurisdiction. It forms a non-negotiable boundary for all planning and action.

Living File The concept that the IPOE product is not a static, finished document, but a dynamic intelligence file that must be continuously updated through the process of **Area Assessment** to

remain relevant.

Modified Combined Obstacle Overlay (MCOO) The primary graphic product for synthesizing terrain analysis. For SC use, it is a map overlay that visually depicts militarily significant aspects of the terrain, including Avenues of Approach, Key Terrain, Obstacles, and terrain mobility classifications (unrestricted, restricted, severely restricted).

Most Dangerous COA The threat Course of Action that, if adopted, would pose the greatest threat to the safety of the ENA community, the success of the SC mission, or the security of SC elements. It may not be the most likely COA.

Most Likely COA The threat Course of Action that, based on intelligence analysis, the threat is most probable to adopt. The primary friendly plan is designed to counter this COA.

Named Area of Interest (NAI) A specific geographic point, area, or information space (e.g., an online forum) where activity—or a lack of activity—will provide a significant clue as to the threat's intentions and will help confirm or deny a specific threat COA. NAIs are depicted on the **Event Template**.

OAKOC / KOCOA An acronym for the military aspects of terrain: **O**bservation and Fields of Fire, **A**venues of Approach, **K**ey Terrain, **O**bstacles, and **C**over and **A**oncealment. It is the primary framework for analyzing the physical terrain.

OODA Loop A model for decision-making consisting of four distinct but interconnected stages: **O**bserve, **O**rient, **D**ecide, and **A**ct. IPOE is the SC's formal methodology for mastering the Observe and Orient phases.

Operational Environment (OE) A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the leader. Deconstructed for analysis by the SC using the **PMESII-PT** framework.

PMESII-PT An acronym for the eight interrelated operational variables that provide a comprehensive framework for analyzing any operational environment: **P**olitical, **M**ilitary, **E**conomic, **S**ocial, **I**nformation, **I**nfrastructure, **P**hysical Environment, and **T**ime.

Protective Power The Security Corps' unique ability to lawfully gain, sustain, and exploit a secure environment for the Euramerican national community through vigilance, presence, information gathering, and defensive readiness. IPOE is a primary enabler of Protective Power.

Security Corps (SC) The formal security and protective organization of the Euramerican National Assembly.

Situation Template (SITEMP) A graphic depiction of a *specific* threat COA as it would likely unfold on the actual terrain of the AO at a critical time and place. It is created by integrating a threat's **Doctrinal Template** with the environmental effects from the **MCOO**.

Threat (SC Context) Any individual, group, organization, or condition that has the *capability* and *intent* to harm the Euramerican national community, undermine ENA interests, disrupt lawful SC operations, or otherwise threaten the safety and stability the SC is sworn to protect.

Threat Model An analytical product created in IPOE Step 3 that provides a baseline understanding of a specific threat, consisting of three components: a graphic **Doctrinal**

Template, a descriptive narrative of their **Tactics and Options**, and a list of their **High-Value Targets (HVTs)**.

Troop Leading Procedures (TLP) The SC's adapted 8-step planning process for small unit leaders, as detailed in SCDP 5-0, *Planning*. The IPOE process provides the critical intelligence inputs for the TLP.

Wargaming A disciplined process used during planning (TLP) where a friendly COA is mentally tested against a prioritized threat COA (usually the Most Likely and Most Dangerous) to identify flaws, develop contingencies, and synchronize actions. The IPOE's **SITEMPs** provide the script for the threat's actions during a wargame.

Appendix B: IPOE Process Checklists

B-1. Purpose

This appendix provides a series of practical checklists for Security Corps leaders and intelligence personnel to use as a guide when conducting the four-step Intelligence Preparation of the Operational Environment process. These checklists are designed to ensure that all critical tasks and considerations for each step are addressed systematically. They serve as a procedural aid and a quality control tool to help standardize our analytical efforts and ensure the final IPOE product is complete, sound, and legally compliant.

These are tools to guide thought, not to replace it. While the checklists outline the essential "what to do," the quality of the final product will always depend on the analyst's critical thinking, judgment, and rigorous adherence to the principles outlined in this doctrine. All activities must be conducted in strict compliance with applicable laws and ENA policies.

Checklist 1: Step 1 - Define the Operational Environment

Purpose: To focus the intelligence effort by defining the mission's scope and boundaries.

Key Questions Answered: *Where is our area of concern? What is our mission? What do we need to learn?*

Task	Status (✓)	Notes / Key Findings
1. Receive and Analyze the Mission		
___	Acknowledge receipt of the order/directive from higher SC/ENA command.	
___	Identify the **Specified Tasks** explicitly stated in the order.	
___	Identify the **Implied Tasks** necessary to accomplish the mission.	
___	Determine the single **Essential Task** for the mission.	
___	Analyze the **Leader's Intent** from the next two higher echelons.	
___	Identify all **Constraints** (things you must do) and **Restraints** (things you cannot do), especially legal ones.	
2. Define Geographic Boundaries		
___	Identify the **Bullseye** (the primary	

	person, place, or asset to be protected/objective).	
___	Delineate the **Area of Operations (AO)** on a map or overlay.	
___	Delineate the broader **Area of Interest (AI)** on a map or overlay.	
3. Identify Significant OE Characteristics (Initial Scan)		
___	Conduct a high-level scan using the **PMESII-PT** framework.	
___	List the 1-2 most significant **Political** factors (e.g., upcoming election, key leaders).	
___	List the 1-2 most significant **Military (LE)** factors (e.g., LE response time, known threat groups).	
___	List the 1-2 most significant **Economic** factors (e.g., major employer, supply chain node).	
___	List the 1-2 most significant **Social** factors (e.g., major fault lines, influential groups).	
___	List the 1-2 most significant **Information** factors (e.g., dominant media outlet, key online forums).	
___	List the 1-2 most significant **Infrastructure** factors (e.g., critical chokepoint, vulnerable utility).	
___	List the 1-2 most significant **Physical Environment** factors (e.g., key terrain, severe weather risk).	
___	List the 1-2 most significant **Time** factors (e.g., upcoming anniversary, major local event).	
4. Identify Intelligence Gaps and Formulate Information Needs		
___	List what is currently **Known** about the situation.	
___	List what is **Unknown** (the intelligence gaps).	

___	Transform the most critical gaps into prioritized **Information Needs** (focused questions).	
End State for Step 1:		**A defined AO/AI, a list of significant characteristics, and prioritized Information Needs.**

Checklist 2: Step 2 - Describe Environmental Effects

Purpose: To analyze how the environment affects both SC and potential threat operations.

Key Question Answered: *How does the environment (physical, information, human) impact everyone's ability to operate?*

Task	Status (✓)	Notes / Key Products
1. Analyze the Physical Environment		
___	Conduct **OAKOC/KOCOA** analysis of the AO.	
___	- Analyze **Observation and Fields of Fire**, including dead space.	
___	- Analyze **Avenues of Approach** (vehicle and foot) and mobility corridors.	
___	- Identify **Key Terrain**.	
___	- Identify **Obstacles** (natural and man-made).	
___	- Analyze **Cover and Concealment**.	
___	Analyze **Weather** effects (visibility, wind, precipitation, temperature).	
___	Produce a simple **Modified Combined Obstacle Overlay (MCOO)**.	Product: MCOO Overlay
___	Produce a **Terrain Effects Matrix**.	Product: Terrain Effects Matrix
___	Produce a **Weather Effects Matrix**.	Product: Weather Effects Matrix
2. Analyze the Information Environment		
___	Analyze the local **Media**	

	Landscape (key outlets, biases, influence).	
___	Map **Formal and Informal Information Networks** (official channels vs. “grapevine”).	
___	Assess the **Online Environment** (key platforms, narratives, hostile propaganda).	
___	Produce a **Combined Information Assessment** (written summary or simple diagram).	Product: Info Assessment
3. Analyze the Human Domain (Social, Political, Economic)		
___	Analyze **Social** factors (demographics, culture, fault lines, objective mapping of ideological groups).	
___	Analyze **Political** factors (formal governance, informal power, **Legal Framework**).	
___	Analyze **Economic** factors (drivers, supply chains, vulnerabilities).	
___	Produce a **Civil Considerations Assessment** (overlay and/or written summary).	Product: Civil Assessment
End State for Step 2:		**A comprehensive, multi-domain understanding of the OE’s effects, captured in key analytical products.**

Checklist 3: Step 3 - Evaluate the Threat

Purpose: To develop a detailed, baseline understanding of each potential threat.

Key Question Answered: *Who is the threat and how do they prefer to operate?*

Task	Status (✓)	Notes / Key Products
1. Identify Threat Characteristics (for each threat group)		
___	Analyze **Composition** (organization, C2, equipment).	

___	Analyze **Disposition** (geographic array, typical locations).	
___	Assess **Strength** (estimated numbers).	
___	Assess **Combat Effectiveness** (training, experience, leadership, morale).	
___	Analyze **Doctrine and Tactics** (ideology and observed TTPs).	
___	Analyze **Support and Relationships** (logistics, funding, recruitment, alliances).	
2. Create Threat Model (for each threat group)		
___	Develop a graphic **Doctrinal Template** for their key actions (e.g., protest, patrol).	Product: Doctrinal Template
___	Write a narrative **Description of Tactics and Options**, including likely branches and sequels.	Product: Narrative Description
___	Identify their **High-Value Targets (HVTs)**, which represent their critical vulnerabilities.	Product: HVT List
End State for Step 3:		**A portfolio of detailed Threat Models for all significant potential threats in the AO/AI.**

Checklist 4: Step 4 - Determine Threat Courses of Action (COAs)

Purpose: To synthesize threat and environmental analysis into predictive intelligence.

Key Question Answered: *What is the threat likely to do here and now?*

Task	Status (✓)	Notes / Key Products
1. Identify Threat Objectives		
___	Determine the threat's likely **Objective(s)** for the specific situation.	
___	Determine the threat's desired **End State**.	

2. Develop the Full Set of Threat COAs		
___	Brainstorm all potential COAs the threat could take.	
___	Test each brainstormed COA against the five validity criteria:	
___	- Is it **Suitable**?	
___	- Is it **Feasible**?	
___	- Is it **Acceptable** (to them)?	
___	- Is it **Unique**?	
___	- Is it **Consistent** with their patterns?	
3. Evaluate and Prioritize Threat COAs		
___	Analyze the full set of valid COAs to determine the **Most Likely COA**.	
___	Analyze the full set of valid COAs to determine the **Most Dangerous COA**.	
4. Develop Priority COAs in Detail		
___	For each priority COA (Most Likely, Most Dangerous), create a **Situation Template (SITEMP)**.	Product: SITEMP Overlays
___	For each priority COA, write a detailed **Threat COA Statement** (Who, What, When, Where, How, Why).	Product: Threat COA Statements
5. Develop Collection Tools		
___	Compare the SITEMPs to identify unique, discriminating activities.	
___	Designate **Named Areas of Interest (NAIs)** based on these differences.	
___	Create the **Event Template** (a graphic overlay of all NAIs).	Product: Event Template
___	Create the **Event Matrix** (a	Product: Event Matrix

	table linking NAIs to specific indicators, times, and the COAs they indicate).	
End State for Step 4:		**A prioritized list of threat COAs and the predictive intelligence tools (SITEMPs, Event Template/Matrix) needed to drive friendly planning.**

Appendix C: Sample IPOE Products

C-1. Purpose

This appendix provides simplified, standardized templates for the key graphical and textual products developed during the Intelligence Preparation of the Operational Environment (IPOE) process. These templates are designed to be practical for Security Corps (SC) use, emphasizing clarity and relevance over excessive complexity. Leaders and intelligence personnel should use these formats as a baseline for creating their own mission-specific products, ensuring consistency and shared understanding across the organization. The quality of the analysis *within* the template is more important than the artistic quality of the graphic itself.

Template 1: SC Modified Combined Obstacle Overlay (MCOO)

Description: The MCOO is the primary graphic for synthesizing terrain analysis (IPOE Step 2). It is a map overlay that visually depicts how the physical terrain will impact the movement of both SC and threat elements. It provides an at-a-glance understanding of the "physical battlefield."

Instructions:

1. Start with a clean base map or satellite image of your Area of Operations (AO).
2. Identify all obstacles (rivers, dense woods, steep slopes, major man-made barriers) and outline them.
3. Based on the cumulative effect of these obstacles, shade or color-code the entire AO according to terrain mobility classifications for a specific force type (e.g., for vehicles).
4. Identify and draw the primary and alternate Avenues of Approach (AAs).
5. Identify and circle the most critical Key Terrain features.
6. Include a legend explaining all symbols and colors.

(Sample MCOO Graphic)

[A sample map graphic would be inserted here. The graphic would show a fictional area with the following elements clearly depicted:]

- **Title Block:**
  - TITLE: MCOO - Liberty County AO
  - DTG PREPARED: 151000Z AUG 20XX
  - PREPARED BY: 1st Squad Intel
- **Base Map Features:** Roads, rivers (e.g., "Freedom River"), key towns (e.g., "Independence"), and major hills (e.g., "Patriot's Ridge").
- **Terrain Mobility Shading:**
  - **Green Cross-Hatching:** Covering swampy areas and very dense forests, labeled "SEVERELY RESTRICTED."
  - **Green Single-Hatching:** Covering hilly, wooded areas, labeled "RESTRICTED."
  - **No Shading:** Covering open fields and the main town area, labeled

"UNRESTRICTED."

- **Avenues of Approach:**
  - A bold blue arrow labeled "PRIMARY AA (I-76)" following the main interstate.
  - A dashed blue arrow labeled "ALTERNATE AA (WEST)" following a network of secondary farm roads.
- **Key Terrain:**
  - A purple circle labeled "**K**" around the "Miller Bridge" over the Freedom River.
  - A purple circle labeled "**K**" around the peak of "Patriot's Ridge."
- **Legend:** A box in the corner clearly explaining what the shading, lines, and symbols represent.

Template 2: SC Threat Model Fact Sheet

Description: The Threat Model is the primary output of IPOE Step 3. It provides a baseline understanding of a specific threat actor, independent of the environment. A separate fact sheet should be created for each significant threat.

Threat Group: Liberty County Minutemen **Date Prepared:** 161200Z AUG 20XX

1. Composition & Disposition:

- **Type:** Right-Wing Militia Group.
- **Organization:** Hierarchical structure with a known Commander and several Team Leaders. Appears to be organized into 3-4 squad-sized elements.
- **Disposition:** Believed to be dispersed throughout rural areas of northern Liberty County. No known fixed headquarters.

2. Strength & Combat Effectiveness:

- **Strength (Est.):** 30-50 active members (Low Confidence).
- **Effectiveness:** Moderate. Leadership and a significant portion of members have prior military experience. They conduct regular, documented paramilitary-style training. Morale appears high. Discipline is generally good at public events.

3. Doctrine & Tactics (TTPs):

- **Doctrine/Ideology:** Constitutionalist / Anti-Federal Government. Stated goal is to "defend the Constitution against all enemies, foreign and domestic."
- **Observed TTPs:**
  - Conduct armed "Show of Force" patrols at political rallies.
  - Provide unofficial "security" for conservative political figures/events.
  - Use specific small-unit movement formations (wedge, file) during patrols.
  - Establish vehicle checkpoints at their private training events.
  - Heavy use of online forums for recruitment and coordination.

4. Support & Relationships:

- **Logistics:** Self-funded through member dues and donations. Members provide their own legal firearms and equipment.
- **Relationships:** Known rivalry with the Liberty Action Collective (Antifa-affiliated). Appear to have some political sympathy from at least one County Commissioner.

5. Graphic Doctrinal Template (Show of Force Patrol):

- [A simple diagram would be inserted here showing a squad-sized element. It would depict:]
  - A point man, followed by a team leader.
  - Two main body elements on either side of the leader.
  - A rear security element.
  - Labels indicating roles and general spacing.

6. Narrative of Tactics and Options (Show of Force Patrol):

- **Objective:** To project strength, deter counter-protestors, and show support for a political cause.
- **Key Tasks:** Maintain formation, provide 360-degree security, project a professional image, report observations to the team leader.
- **Branches (Contingencies):** If verbally harassed, TTP is to hold position and not engage. If physically attacked, TTP is to form a defensive perimeter and use lawful force in self-defense.
- **Sequels (Follow-on):** If the event concludes peacefully, TTP is to conduct an orderly withdrawal to a pre-designated rally point.

7. High-Value Targets (HVTs):

- **Key Leader:** The group's commander, "Bob Jones." His removal would likely disrupt their C2.
- **Key Resource:** The privately-owned farm in western Liberty County used for their training.
- **Key Information Asset:** Their primary online forum, used for recruitment and planning.
- **Key Belief:** Their public image as disciplined "constitutional defenders" rather than an unruly mob.

Template 3: SC Situation Template (SITEMP)

Description: The SITEMP is a key output of IPOE Step 4. It is a graphic overlay that depicts a *specific* threat COA on the actual terrain of the AO at a critical moment.

(Sample SITEMP Graphic)

[A sample map graphic would be inserted here, using the same MCOO base as Template 1.]

- **Title Block:**
  - TITLE: SITEMP - LCM MOST LIKELY COA
  - THREAT COA: Provide armed security for protest at County Courthouse.
  - DTG PREPARED: 171400Z AUG 20XX
- **Base Map/MCOO Features:** Shows the town of "Independence" with the Courthouse as a central feature. Key roads are shown.
- **Threat Dispositions (in Red):**
  - An icon for a **Threat Command Post (CP)** is placed in a nearby park, which offers good concealment.
  - Icons for **Threat Observation Posts (OPs)** are placed on the rooftops of two tall buildings overlooking the courthouse square (Key Terrain).

    - Icons for two **Threat Squads** are shown in formation, establishing a perimeter on the north and south sides of the courthouse.
    - Icons for several **Threat Vehicle Checkpoints (VCPs)** are shown on the secondary roads leading to the courthouse.
- **Threat Scheme of Maneuver:**
    - Red arrows show the planned movement of the squads from an **Assembly Area (AA)** in the park to their perimeter positions.
- **Legend:** A box explaining the red threat symbols.

Template 4: SC Event Template and Event Matrix

Description: These two products are the final output of IPOE Step 4 and are the primary tools for driving the Information Gathering Plan. The Event Template shows *where* to look (NAIs), and the Event Matrix explains *what to look for* (Indicators) and *what it means*.

(Sample Event Template Graphic)

[A sample map graphic would be inserted here, using the same MCOO base.]

- **Title Block:**
    - TITLE: EVENT TEMPLATE - LIBERTY COUNTY PROTEST
    - DTG PREPARED: 180900Z AUG 20XX
- **Base Map Features:** Shows key locations like the Courthouse, the Industrial Park, major roads, etc.
- **Named Areas of Interest (NAIs):**
    - A blue circle labeled "**NAI 1**" is drawn around the County Courthouse square.
    - A blue circle labeled "**NAI 2**" is drawn around a public parking lot two blocks west of the Courthouse.
    - A blue circle labeled "**NAI 3**" is drawn around the main entrance to the Industrial Park on the south side of town.
    - A blue line labeled "**NAI 4**" is drawn along the I-76 overpass at the Miller Bridge.
- **Legend:** Explains that the blue circles/lines are NAIs where key indicators of threat COAs are expected to be observed.

(Sample Event Matrix Table)

EVENT MATRIX - LIBERTY COUNTY PROTEST

NAI	Indicator	Time (H-Hour is 1400)	Threat COA Indicated
NAI 1 (Courthouse)	Presence of >10 Liberty Action Collective members with banners.	H-2 to H-1	COA 1 (Most Likely): Counter-Protest
NAI 2 (Parking Lot)	Staging of >20 Liberty County Minutemen members, forming up for patrol.	H-2 to H-1	COA 1 (Most Likely): Security Patrol
NAI 3 (Industrial	Presence of vehicles carrying tires, lumber, or barrels suitable for a	H-4 to H-2	COA 2 (Most Dangerous): I-76

Park)	blockade.		Blockade
NAI 3 (Industrial Park)	Staging of >15 Liberty Action Collective members wearing black clothing and carrying backpacks.	H-3 to H-1	COA 2 (Most Dangerous): I-76 Blockade
NAI 4 (I-76 Overpass)	Deployment of individuals as lookouts or banner-hangers.	H-1 to H-Hour	Confirms COA 2 (Most Dangerous) is imminent.

Appendix D: Comprehensive PMESII-PT Collection Checklist

D-1. Purpose

This checklist is designed to be a comprehensive, hands-on tool to guide the collection phase of the Intelligence Preparation of the Operational Environment (IPOE) process. It provides a detailed list of questions and data points organized by the PMESII-PT framework. Its purpose is to prompt thorough research and ensure that no critical aspect of the operational environment is overlooked.

D-2. How to Use This Checklist

It is not necessary or practical to answer every single question on this list for every mission. The required level of detail will be dictated by the specific mission, the time available, and the leader's Information Needs. Use this checklist as a master guide:

1. **During Step 1 (Define OE):** Review this list to help brainstorm the significant characteristics of your AO/AI and to formulate your initial Information Needs.
2. **During Step 2 (Describe Effects):** Use the relevant sections as a detailed "shopping list" for data collection on the physical, information, and human domains.
3. **During Continuous Assessment:** Refer back to this list periodically to identify gaps that may have emerged in your knowledge and to guide the updating of your living intelligence file.

(P) - Political

Formal Governance:

- [ ] What are the precise boundaries of my city, county, and state/federal representative districts?
- [ ] Who are the current key elected officials at the municipal, county, and state levels (Mayor, Commissioners, Sheriff, Governor, State Representatives, etc.)?
- [ ] What are their political party affiliations, term lengths, and key policy positions relevant to my goals?
- [ ] What is the structure of the local government (e.g., Mayor-Council, Council-Manager)? Who holds the primary executive authority?

Informal Governance & Influence:

- [ ] Who are the most influential non-elected individuals in the AO (e.g., major business owners, wealthy philanthropists, influential community activists, leaders of prominent families)?
- [ ] What non-governmental groups (e.g., Chamber of Commerce, labor unions, taxpayer associations) hold significant political sway?
- [ ] Who are the major donors to local political campaigns?

Political Activism & Extremism:

- [ ] How do the ideological groups identified in the Social domain interact with the formal political system?
- [ ] Which candidates or policies do they actively support or oppose?
- [ ] What is the historical relationship between these groups and local law enforcement during political events?

Legal Framework:

- [ ] Who has the legal authority to declare a local or state State of Emergency?
- [ ] What specific powers are granted to the government under a State of Emergency (e.g., curfews, travel restrictions, confiscation of property)?
- [ ] What are the specific state and local laws regarding self-defense, including “Castle Doctrine” and “Stand Your Ground” provisions?
- [ ] What are the state and local laws governing the possession and transport of firearms and other defensive tools (e.g., body armor, knives, batons)?
- [ ] What are the local ordinances regarding public assembly, protests, and what constitutes an “unlawful assembly”?
- [ ] What are the state laws regarding video and audio surveillance/recording (one-party vs. two-party consent)?

(M) - Military (Law Enforcement & Emergency Services)

Law Enforcement:

- [ ] What are the precise jurisdictional boundaries for the City Police, County Sheriff, and State Police?
- [ ] Where are the physical locations of their stations, headquarters, and barracks?
- [ ] What is the average response time for my specific location?
- [ ] What is the approximate number of sworn officers in each department?
- [ ] Do the local agencies have specialized units (e.g., SWAT, K9, Bomb Squad)?
- [ ] What is the agency’s historical posture regarding civil unrest (e.g., passive monitoring vs. active enforcement)?

Military Presence:

- [ ] Are there any Active, Reserve, or National Guard bases, armories, or facilities in the AO/AI? Where are they?
- [ ] What are the primary units stationed at these facilities (e.g., logistics, infantry, engineering)?
- [ ] What is the primary role of the local National Guard unit(s), and under what circumstances can the Governor activate them?

Emergency Services:

- [ ] Where is every fire station located in the AO? Are they professional or volunteer?
- [ ] Who is the primary EMS/ambulance provider? Where are their stations?
- [ ] Where is the county’s Emergency Operations Center (EOC) located?

(E) - Economic

Economic Drivers:

- [ ] What are the top 3-5 major industries that fuel the local economy?
- [ ] Who are the top 5-10 largest single employers in the county?
- [ ] If rural, what are the primary agricultural products and what is the seasonal cycle (planting, harvest)?
- [ ] Is the economy diverse, or is it heavily dependent on a single industry or employer?

Logistics & Supply Chain:

- [ ] Where are the major logistics and distribution centers (food, retail) that service the AO?
- [ ] Where are the major commercial rail lines, freight yards, and industrial parks?
- [ ] Where are the major retail hubs (clusters of grocery stores, hardware stores, pharmacies)?
- [ ] What are the primary road and rail routes used by commercial logistics?

Financial Infrastructure:

- [ ] Where are the major banks and credit unions located?
- [ ] Are any of these banks headquartered locally?

Economic Vulnerabilities:

- [ ] How susceptible is the AO to a major disruption in the national supply chain?
- [ ] What would be the effect of the largest employer shutting down?
- [ ] Is there evidence of a significant black or grey market economy?

(S) - Social

Demographics:

- [ ] What is the total population of the AO? Where is it most densely concentrated?
- [ ] What is the median age, median household income, and poverty rate?
- [ ] What is the racial and ethnic composition of the AO? Are there distinct enclaves?

Culture & Religion:

- [ ] What are the dominant cultural norms and values (e.g., conservative/liberal, rural/urban)?
- [ ] What are the largest and most influential religious denominations and congregations?
- [ ] Where are the key community gathering centers (churches, community halls, VFW posts)?
- [ ] What are the major annual fairs, festivals, or traditions?

Social Cohesion & Division:

- [ ] What are the primary social fault lines (e.g., economic, political, racial, old vs. new residents)?
- [ ] Who are the key formal and informal power brokers and community leaders?
- [ ] What are the major civic and volunteer groups (Rotary, Lions, etc.)?

Ideological & Extremist Groups:

- [ ] What specific left-wing groups (e.g., Antifa networks, socialist organizations) are known to be active in the AO/AI?
- [ ] What are their stated goals, typical tactics, and primary operating areas?
- [ ] What specific right-wing groups (e.g., militias, sovereign citizens, white supremacist organizations) are known to be active in the AO/AI?
- [ ] What are their stated goals, typical tactics, and primary operating areas?
- [ ] Has there been a history of clashes between these groups? Where and when did they occur?

Health & Medical:

- [ ] Where are all the hospitals located? What are their trauma level designations?
- [ ] Where are the urgent care clinics, public health clinics, and major pharmacies?
- [ ] Is the medical system robust, or is it vulnerable (e.g., only one hospital for a large area)?

(I) - Information

Media Landscape:

- [ ] What are the dominant local news sources (TV, radio, newspaper, major blogs)?
- [ ] What are their general political leanings and levels of credibility?
- [ ] What are the most popular news/talk radio stations?

Formal & Informal Networks:

- [ ] What are the official emergency alert systems for the county/state?
- [ ] Where are the physical or digital “town squares” where information and rumors spread?
- [ ] Who are the key local “influencers” on social media?

Online Information Environment:

- [ ] What platforms are used by local activist/extremist groups for propaganda and mobilization?
- [ ] What are the dominant narratives and conspiracy theories circulating locally online?

Language & Literacy:

- [ ] Are there significant non-English speaking populations? What languages do they speak?
- [ ] Could language barriers impede the dissemination of emergency alerts?

(I) - Infrastructure

Transportation:

- [ ] What are the primary (interstate), secondary (state/county), and tertiary (local/unimproved) roads?
- [ ] Where is every key chokepoint (bridge, tunnel, major intersection, rail crossing)? What are their conditions and limitations (e.g., weight limits, clearance heights)?

- [ ] Where are the local airports, private airstrips, and rail lines?

Energy:

- [ ] Where are the power plants that service the AO?
- [ ] Where are the major electrical transmission lines and substations?
- [ ] Where are the bulk storage facilities for natural gas, gasoline, and propane?

Water & Sanitation:

- [ ] Where is the water treatment plant? Where are the major water towers and pumping stations?
- [ ] Where is the wastewater (sewage) treatment plant?
- [ ] What is the primary source of municipal water (river, reservoir, aquifer)?

Communications:

- [ ] Where are the major cell phone towers located in the AO?
- [ ] Are there known communications dead zones?
- [ ] Where are the major fiber optic cable routes and telephone company central offices?

(P) - Physical Environment

Topography (OAKOC/KOCOA):

- [ ] What are the highest and lowest points of elevation in my AO?
- [ ] Where are the major ridgelines, hills, and valleys that affect observation and movement?
- [ ] What areas have a steep slope that would inhibit vehicle or foot traffic?
- [ ] Where are the large, flat, open areas that offer good fields of fire but poor concealment?

Hydrography:

- [ ] Where are the major rivers, lakes, and streams? In which direction do they flow?
- [ ] Where are all the bridges, dams, and major fords that cross these water features?
- [ ] What areas are designated as 100-year or 500-year flood plains by FEMA?
- [ ] What are potential secondary sources of fresh water?

Climate & Weather:

- [ ] What are the average high/low temperatures and precipitation for each month?
- [ ] What is the prevailing wind direction?
- [ ] What are the most likely and most dangerous severe weather threats for the AO (e.g., tornadoes, hurricanes, blizzards, ice storms, wildfires, droughts)?
- [ ] What is the peak season for each of these severe weather threats?

(T) - Time

Rhythms & Cycles:

- [ ] What are the daily rush hour patterns?
- [ ] What are the weekly patterns (e.g., weekend traffic to a recreational area)?

- [ ] What are the seasonal patterns that affect activity (e.g., harvest, tourist season, winter storms)?

Historical Context:

- [ ] Are there any significant historical events that still shape local politics and attitudes?
- [ ] What are the key anniversaries that might be a catalyst for planned events or protests?

Tempo & Timing:

- [ ] How long does it take for emergency services to respond to my specific location?
- [ ] How long would it take to evacuate the AO during normal traffic versus a crisis?
- [ ] What is the timeline for predictable events (e.g., the annual county fair always occurs on the third week of August)?

Appendix E: Legal Compliance in IPOE Reminder

E-1. The Non-Negotiable Foundation

This appendix serves as an essential and unwavering reminder to every member of the Euramerican Security Corps (SC): **Absolute compliance with applicable law is the non-negotiable foundation of all intelligence activities.**

The doctrine and methodologies in this publication are designed to function *within*, and are entirely subordinate to, the framework of established law in every jurisdiction where we operate. No operational objective, perceived necessity, or order from any leader can ever justify or excuse actions that violate applicable federal, state, or local laws and regulations. Our legitimacy, our operational freedom, and the very safety of our members depend on our disciplined adherence to this principle.

E-2. Core Principles of Lawful Intelligence Gathering

- **Legality is the Overriding Principle.** Every intelligence activity, from initial planning to final dissemination, must be filtered through the question: “Is this lawful?” If the answer is anything other than a confident “Yes,” the action must not be taken.
- **Ignorance of the Law is Not a Defense.** It is the responsibility of every SC leader and member to understand the basic legal boundaries relevant to their duties. Claiming you “didn’t know” is not an acceptable excuse for an unlawful act.
- **Jurisdiction is Key.** Laws regarding surveillance, privacy, and the use of certain equipment can vary dramatically from one state or county to the next. A method that is lawful in one Area of Operations may be a felony in another. All intelligence planning must be specific to the jurisdiction of the operation.
- **When in Doubt, Seek Guidance.** If there is *any* ambiguity or uncertainty about the legality of a proposed action, you have a duty to halt and seek clarification. This must be done through the SC chain of command, which will consult with designated Euramerican National Assembly (ENA) legal counsel. Do not guess.

E-3. Strictly Prohibited Activities

The following activities are **strictly forbidden** for all SC personnel engaged in any intelligence or information gathering function:

1. **NO Illegal Surveillance or Interception.** This includes, but is not limited to, illegal wiretapping, intercepting private emails or text messages, and using listening devices to monitor private conversations.
2. **NO Unauthorized Physical Intrusion.** This includes trespassing on private property, conducting unauthorized searches of vehicles or buildings, or installing surveillance devices on private property without lawful consent.
3. **NO Hacking or Unauthorized Digital Access.** This includes attempting to bypass password protections, accessing private online accounts or computer systems without permission, or using malware or other illegal means to obtain digital information.

4. **NO Coercion, Deception, or Misrepresentation.** Information from human sources must be obtained voluntarily and ethically. The use of threats, intimidation, blackmail, or deception (e.g., creating fake online profiles to gain access to private groups, misrepresenting your identity or purpose) is prohibited.
5. **NO Unlawful Recording.** You must know and strictly adhere to the specific state laws regarding the recording of audio and video conversations (i.e., one-party vs. two-party consent laws). Unlawful recording is a serious crime.
6. **NO Possession or Use of Illegal Equipment.** The possession or use of any equipment that is illegal in the specific jurisdiction—be it a specific type of electronic device, a prohibited defensive tool, or any other item—is forbidden.

E-4. Specific Considerations for Key Collection Activities

- **Open Source Intelligence (OSINT):** Lawful does not mean limitless. Your collection is restricted to publicly available information. You must respect website terms of service, copyright laws, and the privacy settings of individuals on social media. Do not attempt to access private, "friends-only" information or use deceptive means to do so.
- **Human Intelligence (HUMINT):** All interaction must be voluntary and ethical. You may ask questions, but individuals are free to refuse to answer. You must not pressure or harass them. Any information shared must be handled with the utmost discretion, particularly if it involves the privacy of other community members.
- **Unmanned Systems (UxS/Drones):** The operation of UxS for observation is a legally complex area. All flights must strictly comply with a "triple check" of:

Aviation Regulations (e.g., FAA rules in the US).
State and Local Privacy Laws (regarding surveillance of private property).
Specific Local Ordinances that may restrict drone use.

E-5. The Leader's Responsibility

Leaders at all levels are personally responsible for ensuring the legality of the intelligence activities conducted by their elements. This responsibility includes:

- Proactively researching or seeking guidance on the legal framework for any planned operation.
- Ensuring that all plans, orders, and briefings explicitly address legal constraints and ROE.
- Supervising execution to prevent unlawful actions by subordinates.
- Immediately halting any activity that is or may become unlawful.

E-6. Final Admonition

The Security Corps exists to provide lawful protection. Operating outside the law fundamentally contradicts our purpose, violates our Core Beliefs, and serves only the interests of those who would see our community harmed and our organization delegitimized. Violations of the law will not be tolerated and will expose the individual member, their leaders, and the SC to severe consequences, including criminal prosecution and civil liability.

Legitimacy is our shield; lawfulness is our guidepost.